

SANDIA REPORT

SAND2005-2348P

Unlimited Release

Printed April 2005

Laboratory Biosecurity Implementation Guidelines

Chemical and Biological Weapons Nonproliferation Department 6928

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401

Facsimile: (865)576-5728

E-Mail: reports@adonis.osti.gov

Online ordering: <http://www.doe.gov/bridge>

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847

Facsimile: (703)605-6900

E-Mail: orders@ntis.fedworld.gov

Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>



SAND 2005-2348P
Unlimited Release
Printed April 2005

Laboratory Biosecurity Implementation Guidelines

Chemical and Biological Weapons Nonproliferation Department 6928
Sandia National Laboratories
Albuquerque, NM 87185-1371

Abstract

In 2004, the World Health Organization published the third edition of its *Laboratory Biosafety Manual (LBM)*. The third edition of the *LBM* for the first time included a chapter on “Laboratory Biosecurity Concepts.” The intent of this Sandia document, *Laboratory Biosecurity Implementation Guidelines*, is to provide guidance to bioscience facilities on the implementation of the laboratory biosecurity concepts first introduced in the third edition of the *LBM*. Biosafety and biosecurity are both critical and should be integrated as seamlessly as possible in the operations of the modern bioscience laboratory. After a brief discussion of the common components and potential conflicts between biosafety and biosecurity, this document focuses on the fundamentals for biosecurity: risk, physical security, personnel management, material control and accountability, and programme management. A risk assessment is the fundamental resource allocation step and serves as the foundation for the design of a rational, facility-specific biosecurity program. Management should use the results of the risk assessment to decide on a protection strategy that allows for a graded implementation of biosecurity based on the risk.

DISCLAIMER

In 2004, the World Health Organization (WHO) requested that the Sandia National Laboratories (SNL) Biosecurity Team draft laboratory biosecurity implementation guidelines that could be understood and implemented by the global public health community. It was expected that, in many cases, the public health facilities within WHO Member States would be unfamiliar with laboratory biosecurity and would have limited resources to allocate for biosecurity. The WHO advised SNL that, because the WHO has no authority to enforce laboratory biosecurity implementation, the guidelines should not be prescriptive. Additionally, SNL was asked to minimize Western approaches to security because the WHO must gain consensus from its Member States from all over the globe. As a result, the SNL Biosecurity Team compromised the normal stringency of its biosecurity recommendations in order to accommodate the customer and the customer’s audience.

This page intentionally left blank.

Contents

List of Acronyms	9
1. Introduction	11
1.1 Risk Posed by Natural and Deliberate Outbreaks of Highly Infectious Diseases	11
1.2 Benefits of Laboratory Biosecurity	12
1.3 The Concept of Laboratory Biosecurity: Balancing Security and Research	12
1.4 Challenges Associated with Protecting Pathogens and Toxins	13
1.5 Laboratory Biosecurity Risk Assessment	14
1.6 Components of a Laboratory Biosecurity System	14
1.7 Achieving Global Laboratory Biosecurity	16
2. Laboratory Biosafety and Laboratory Biosecurity	17
2.1 Defining Laboratory Biosecurity and Laboratory Biosafety	17
2.2 Common Components of Laboratory Biosecurity and Laboratory Biosafety	17
2.3 Ways That Laboratory Biosafety Contributes to Laboratory Biosecurity	18
2.4 Potential Conflicts between Biosafety and Biosecurity	19
2.5 Combined Strength of Biosafety and Biosecurity	20
3. Risk	21
3.1 Introduction	21
3.2 Threat Assessment	21
3.3 Consequences	22
3.4 Baseline Risk	23
3.4.1 Baseline Risk Levels for Pathogens and Toxins	23
3.5 Additional Risk Factors	25
4. Physical Security	27
4.1 Introduction	27
4.2 Graded Physical Security	27
4.2.1 Property Protection Area	28
4.2.2 Limited Area	28
4.2.3 Exclusion Area	29
4.3 Intrusion Detection	29
4.4 Alarm Assessment	30
4.5 Response Capability	30
4.5.1 On-Site Guard Force	31
4.5.2 Local Law Enforcement	31
4.6 Structural Issues	32
4.7 Electronic Access Control and Intrusion Detection Systems	32
4.8 Performance Testing	33
4.9 Physical Security Policies and Procedures	33
4.9.1 Policies	34
4.9.2 Procedures	34
4.10 Information Security	37

5. Personnel Management	39
5.1 Personnel Suitability	39
5.2 Position Risk	39
5.2.1 Low Risk	39
5.2.2 Moderate Risk	40
5.2.3 High Risk	40
5.3 Employment Screening	41
5.3.1 Pre-Qualification	41
5.3.2 Employment Screening	42
5.3.3 Visitor Screening	42
5.3.4 Interim Access Authorization	42
5.3.5 Screening Updates	43
5.3.6 Derogatory Information	43
5.4 Visitor Control	44
5.4.1 Personal Visitors	44
5.4.2 Working Visitors	44
5.4.3 Limited Areas	45
5.4.4 Exclusion Areas	45
5.4.5 Unescorted Visitor Access	45
5.4.6 Host Responsibilities	45
5.4.7 Escorting	46
5.5 Badges	47
5.6 Employee Assistance Programmes	48
5.7 In-Processing	49
5.8 Out-Processing	49
5.8.1 Access Changes	49
5.8.2 Termination of Access	50
5.9 Counterintelligence Awareness Training	51
5.10 Security Infractions	51
5.11 Information Security	53
6. Material Control and Accountability	55
6.1 Introduction	55
6.2 Materials	56
6.2.1 Agent	56
6.2.2 Quantity	57
6.2.3 Form	57
6.2.4 Detail	58
6.2.5 Required Information	58
6.3 Control Measures	59
6.3.1 Confine Materials to Restricted Areas	59
6.3.2 Material Identification	60
6.3.3 Material Disposition	60
6.3.4 Physical Inventory Taking	60
6.4 Accountability	60
6.4.1 Accountable Scientist	61

6.4.2	MCA Records	61
6.4.3	Timeliness and Historical Archive	62
6.5	Low, Moderate, and High Risk Pathogens and Toxins	63
6.5.1	LRPT	63
6.5.2	MRPT	63
6.5.3	HRPT	63
6.6	Additional Good Practices for External Transfers	64
6.7	Reporting and Review	65
6.8	Transfer/Transport	65
6.9	Information Security	65
7.	Programme Management.....	67
7.1	Management Responsibilities	67
7.2	Programme Planning.....	67
7.3	Roles and Responsibilities	69
7.3.1	Laboratory Director	69
7.3.2	Laboratory Biosecurity Officer.....	69
7.3.3	Personnel Management.....	69
7.3.4	Information Security System Administrator.....	70
7.3.5	Line Managers	70
7.3.6	Individual Researchers and Diagnosticians	71
7.3.7	Response Force Team	71
7.3.8	All Personnel.....	71
7.4	Laboratory Biosecurity Training	72
7.4.1	Annual Comprehensive Training.....	72
7.4.2	Annual Supervisory Training.....	73
7.4.3	Annual Response Force Training	74
7.5	Self-Assessments	74
7.5.1	Programme Management.....	75
7.5.2	Physical Security.....	75
7.5.3	Personnel Management.....	75
7.5.4	Material Control and Accountability	75
7.5.5	Corrective Action Plans	75
Appendix A. Information Security.....		77
Appendix B. Network Security		81
Appendix C. Biosecurity by Baseline Risk Category.....		87
Appendix D. Adversary Descriptions.....		96

Figures

Figure 1.	Graded Protection Areas	28
-----------	-------------------------------	----

This page intentionally left blank.

List of Acronyms

BSL	biosafety level (refers to levels of containment for laboratories - the most dangerous organisms from a safety perspective are in BSL 4)
EAP	employee assistance programme
ERPT	extreme risk pathogens and toxins
FMD	foot and mouth disease
GAO	Government Accountability Office (US)
DC	District of Columbia
HEPA	High Efficiency Particulate Air (filter)
HRPT	high risk pathogens and toxins
LAN	local area network
<i>LBM</i>	<i>Laboratory Biosafety Manual</i> (WHO)
LRPT	low risk pathogens and toxins
MCA	material control and accountability
MRPT	moderate risk pathogens and toxins
NM	New Mexico
PDA	personal data assistant
PIN	personal identification number
PIT	physical inventory taking
SARS	severe acute respiratory syndrome
SNL	Sandia National Laboratories
US	United States
vLAN	virtual LAN
VPN	virtual private network
WHO	World Health Organization

This page intentionally left blank.

1. Introduction

1.1 Risk Posed by Natural and Deliberate Outbreaks of Highly Infectious Diseases

Recent natural outbreaks of highly infectious disease have had devastating consequences for public and agricultural health, the international economy, and international security.¹ The outbreak of severe acute respiratory syndrome (SARS) that started in Asia in 2003 infected over 8,000 people and killed almost 800, ravaged economies in the Pacific Rim and Canada, and struck fear across the globe.² The outbreak of foot and mouth disease (FMD) in the United Kingdom in 2001 caused economic losses of approximately 11 billion euros.³ Outbreaks of a zoonotic form of avian influenza in 2004 have also inflicted enormous losses on many Asian countries, and the recovery from these outbreaks is expected to cost approximately 400 million euros.⁴

The consequences of an outbreak of infectious disease resulting from the deliberate, malicious use of a pathogenic microorganism or toxin would be at least as damaging as a naturally occurring infectious disease and possibly more so. The 2001 anthrax attacks in the United States killed five people and injured twenty-two, resulted in enormous economic damage, and brought the issue to the centre of debates on international security. If an agent that causes a highly contagious disease—such as smallpox or FMD—were maliciously deployed in a widespread manner, the international economic and security consequences could be catastrophic.

The risk of infectious disease resulting from the malicious use of pathogenic microorganisms and toxins is real and growing. The rapid expansion of the biotechnology industry has resulted in the global proliferation of dual-use materials, technologies, and expertise. Thus, the means to create a deliberate epidemic are much more accessible to a wide range of proliferators, including terrorists.

Currently, many different methods are being used to address these global biological risks. Most strategies, such as increasing the effectiveness and availability of therapeutics, improving diagnostic capabilities, and developing decontamination and detection technologies, focus on enhancing national responses to an outbreak of infectious disease after it has occurred.

The international community has also implemented some preventive strategies to address these global biological risks. Preventive strategies are important because they provide an opportunity to counter the threat before it results in an outbreak of disease that must be mitigated by emergency responders and public health officials. A comprehensive strategy to counter the

¹ Mark S. Smolinski, Margaret A. Hamburg, and Joshua Lederberg, *Microbial Threats to Health: Emergence, Detection, and Response* (Washington, DC: 2003).

² U.S. Government Accountability Office (GAO), *Emerging Infectious Diseases: Asian SARS Outbreak Challenged International and National Responses*, GAO-04-564 (April 2004).

³ Report by the Comptroller and Auditor General, *The 2001 Outbreak of Foot and Mouth Disease*, HC 939 2001-2002 (London: June 21, 2002).

⁴ “Asia’s Avian Flu Battle Likely to be Long, Costly,” *CIDRAP News*, (March 1, 2004) <http://www.cidrap.umn.edu/cidrap/content/hot/avianflu/news/mar0104avian.html>.

threat of both natural and deliberate causes of infectious disease should combine identification and response techniques with preventive measures.

One of the principal preventive strategies is laboratory biosecurity: the protection of dangerous pathogens and toxins from theft at the facilities where they are legitimately used and stored. Laboratory biosecurity is achieved by instituting a culture of responsibility and accountability among those who handle, use, transport, and oversee work with dangerous pathogens and toxins.

Ultimately, for laboratory biosecurity to succeed in reducing the risk of deliberate epidemics, it must be implemented globally. Protecting dangerous biological materials in some areas of the world and not in others will not adequately reduce the risk.⁵

1.2 Benefits of Laboratory Biosecurity

Laboratory biosecurity offers numerous benefits. Primarily, laboratory biosecurity helps reduce the risk that dangerous biological materials would be used to cause a deliberate epidemic. As such, laboratory biosecurity provides an important complement to the laboratory biosafety agenda, which aims to prevent *accidental* exposure to or release of harmful microorganisms and toxins from a laboratory.

Laboratory biosecurity also provides assurance to citizens and investors about the security of dangerous pathogens and toxins. Citizens, particularly those in the vicinity of a biological containment laboratory, sometimes worry that disease-causing agents will be released into the community. Potential investors in biotechnology ventures may fear that their investments will somehow be tied to a deliberate use of a pathogen or toxin or that their facilities are perceived as being unsafe or insecure. These issues may introduce excessive liabilities for these investors. By establishing consistent and transparent laboratory biosecurity practices, both citizens and investors can be assured that appropriate steps have been taken to reduce the risk that dangerous pathogens and toxins in these facilities will be misused.

Laboratory biosecurity also plays a valuable role in securing intellectual property that resides in specific samples of dangerous biological materials. By promoting sound laboratory biosecurity practices, researchers can be assured that critical experiments will continue without significant risk of theft.

1.3 The Concept of Laboratory Biosecurity: Balancing Security and Research

The best defence against emerging infectious disease and bioterrorism is the progress of research that results in improved vaccines, diagnostics, and therapies—work that requires handling, using, and transporting dangerous pathogens and toxins. Although some of these agents have the

⁵ Jonathan B. Tucker, “Biosecurity: Limiting Terrorist Access to Deadly Pathogens,” *Peaceworks* No. 52, United States Institute of Peace (Washington, DC: November 2003).

potential to cause serious harm to the health and economy of a population if misused, all have legitimate uses for medical, commercial, and defensive applications.

It is incumbent on those in the scientific community who strive to improve human, animal, and plant health to take measures to limit the opportunities for their valuable materials to be used illicitly. However, it is critically important to strike an appropriate balance between protection of dangerous pathogens and toxins and preservation of an environment that promotes legitimate, ultimately life-saving, biological research.^{6,7}

1.4 Challenges Associated with Protecting Pathogens and Toxins

Designing a laboratory biosecurity system that does not jeopardize microbiological operations requires a familiarity with bioscience and the biological materials that require protection. Security system designers must be cognizant of several challenges to protecting microorganisms and toxins.⁸ First, the biological materials that laboratory biosecurity aims to protect exist in nature and are globally distributed in research laboratories, collection centres, biotechnology institutes, and clinical facilities.⁹ Therefore, any attempt to implement laboratory biosecurity, even on a broad scale, cannot encompass all dangerous biological materials. While this fact must be acknowledged, known collections of viable and virulent pathogens and toxins should be protected so that they do not become potential sources of biological weapons material for someone who is interested in deliberately introducing and spreading infectious disease.

Many other challenges to protecting biological materials exist. Biological agents are living, reproducing organisms. These organisms and the toxins some of them produce can vary in quantity and quality over the course of legitimate research activities as a result of growth, death, and mutation of the organisms. Therefore, knowing exactly how much dangerous biological material is located within a given biological sciences facility and the exact nature of that material is not achievable.

Within bioscience facilities, biological agents can be isolated from a number of process streams. They can be found in Petri dishes, cell cultures, environmental samples, clinical specimens, and infected animals and animal carcasses as well as stored in refrigerated or freeze-dried forms. This wide distribution makes safeguarding all of the material a complicated task. Technology does not exist that can detect someone leaving a facility with a small amount of an organism hidden in his clothing or his bags, nor can the naked eye identify usable amounts of a pathogen.

⁶ Jennifer Gaudioso and Reynolds M. Salerno, "A Conceptual Framework for Biosecurity Levels," *BTR 2004: Unified Science and Technology for Reducing Biological Threats and Countering Terrorism-Proceedings* (Albuquerque, NM: March 2004). (<http://www.biosecurity.sandia.gov/documents/conceptual-framework-biosecurity-levels.pdf>)

⁷ Reynolds M. Salerno, Natalie Barnett, and Jennifer Koelm, "Balancing Security and Research at Biomedical and Bioscience Laboratories," *BTR 2003: Unified Science and Technology for Reducing Biological Threats and Countering Terrorism-Proceedings* (Albuquerque, NM: March 2003). (<http://www.biosecurity.sandia.gov/documents/balancing-security-and-research.pdf>)

⁸ National Research Council of the National Academies, *Biotechnology Research in an Age of Terrorism: Confronting the Dual Use Dilemma* (Washington, DC: October 2003).

⁹ The one exception is the Variola major virus, the causative agent of smallpox, which has been globally eradicated. The two official WHO repositories are the Centers for Disease Control and Prevention, Atlanta, Georgia (US) and the State Research Institute for Virology and Biotechnology, Koltsovo (Russia).

Therefore, intercepting someone who is in the midst of covertly removing biological material from a laboratory is almost impossible.

1.5 Laboratory Biosecurity Risk Assessment

These challenges compel laboratory biosecurity system designers and laboratory managers to think carefully about what form of security will be effective in securing dangerous biological materials from theft. Those responsible for the safekeeping of these materials must understand that security risks are impossible to eliminate; they can only be mitigated. Since security in a biological environment can never be perfect, it is incumbent upon security system designers to employ a risk management approach.

A risk management approach to laboratory biosecurity recognizes that different assets at an institution may represent different levels of security risk. These risks need to be prioritized through a risk assessment process. Those assets at the highest risk should receive the most protection, and lower risk assets should receive commensurately less protection. The allocation of resources and the implementation of operational restrictions should be at the discretion of facility management, but the application should always be in a graded manner—protecting the assets at the highest risk more than those at lower risks.

Risk assessment begins by identifying the facility's assets. For the purposes of these guidelines, the principal assets of concern are dangerous pathogens and toxins. The consequences that could result from the theft of these assets, such as use as a biological weapon, represent one critical component of the risk. The likelihood that an adversary might attempt to execute such an act of theft represents another critical component of risk. Specifically, risk is a function of the relationship between the consequences of an undesired event (theft) and the likelihood, or threat potential, posed by an adversary. As the threat potential and the consequences increase, so does the risk. The risk may be mitigated with security measures that reduce the adversary's likelihood of success. Although biosecurity can reduce the risk of theft, these measures cannot eliminate the risk.

1.6 Components of a Laboratory Biosecurity System

An effective laboratory biosecurity system includes many different components and does not rely on physical security and technologies alone. In fact, the most important aspects of a laboratory biosecurity system are procedural and cultural—elements that do not require large expenditures of resources. For example, a laboratory biosecurity system should physically consolidate, to the extent possible, all dangerous pathogens and toxins. Access to these areas should then be controlled, and the number of personnel who are authorized to handle, use, and transport these materials should be limited.

Personnel should receive authorization, based on legitimate need and appropriate screening, to enter areas where dangerous pathogens or toxins are used or stored. Those authorized personnel should be regularly trained in both laboratory biosafety and laboratory biosecurity and should only handle, use, or transfer those specific materials as necessary to fulfill their assigned

laboratory duties. Procedures should be established for escorting visitors and support personnel who only need occasional access to areas where dangerous pathogens or toxins are located.

A laboratory biosecurity system should also establish a means to control and maintain accountability for dangerous pathogens and toxins, both within the laboratory and during transfer. Material control and accountability (MCA) procedures should avoid applying rigorous quantitative inventory accounting principles, which are impossible to achieve in a biological environment. Instead, procedures should focus on documenting exactly which dangerous pathogens and toxins exist at the facility, where in the facility they are located, who has access to them, and who is responsible for them. Because dangerous pathogens and toxins are often transferred between facilities and shared among researchers, it is important for a laboratory biosecurity system to include procedures for documenting and controlling both internal and external transfers of these materials. Ideally, these procedures should demonstrate continuous custody by authorized individuals throughout the transfer process.

All of the components of the laboratory biosecurity system should be documented in a laboratory biosecurity plan, which should be regularly reviewed and revised by the facility's management. An incident response plan should also be written to address potential emergency situations, including those security risks judged to be too low to warrant extensive investment in protection measures. The incident response plan should be regularly reviewed and revised based on consultations between the facility's management and local response forces that can support the facility's biosecurity system.

These core and other security-related documents require protection from unauthorized access, because they could be used to facilitate malicious acquisition of dangerous pathogens and toxins. Thus, laboratory biosecurity systems should also include procedures for handling, using, and storing certain sensitive information related to the protection of dangerous pathogens and toxins.

Facility management should ensure that all components of the laboratory biosecurity system function optimally. To do this, management will assume responsibility for developing and maintaining the laboratory biosecurity and incident response plans, conducting regular security training for the institution's staff, and creating and sustaining a laboratory biosecurity culture for the institution.

It is important to note that an appropriate level of laboratory biosecurity can be achieved without relying on expensive technologies or unusually burdensome procedures. Although some countries have chosen to enact relatively strict laboratory biosecurity regulations, this degree of rigor may not be necessary to achieve global laboratory biosecurity. Laboratory biosecurity implementations will vary depending on the risks various institutions and countries have the level of risk aversion or risk tolerance each facility or country has, and the availability of resources. Careful consideration of the particular needs of each country and facility will be essential to achieving a broad-based global implementation of laboratory biosecurity.

1.7 Achieving Global Laboratory Biosecurity

The risk posed by natural and deliberate outbreaks of highly infectious disease is significant and demands a coordinated and global strategy to reduce the likelihood that a devastating or highly disruptive event could occur. One component of this strategy is laboratory biosecurity, the protection of dangerous pathogens from theft at legitimate bioscience facilities. If implemented globally, laboratory biosecurity could significantly reduce the risk of deliberately introduced infectious disease and biological weapons proliferation.

The challenges of securing biological materials should compel facility managers to design and sustain a laboratory biosecurity system in accordance with the principles of risk management. Such an approach would help ensure that the amount of protection provided to a specific asset and the cost for that protection are proportional to the risk of theft of that asset. Moreover, laboratory biosecurity risk management should recognize that the most important measures for protecting dangerous pathogens and toxins at a facility are procedural and should not require vast expenditures of resources. Most importantly, laboratory biosecurity risk management should achieve a system that strikes a balance between protection of biological material that could be used maliciously and preservation of an environment that promotes legitimate and lifesaving microbiological research.

Ultimately, making laboratory biosecurity effective will depend on the scientific community. Scientists' and technicians' knowledge of the unique nature of biological materials, research, and operations is essential for the development and implementation of effective laboratory biosecurity practices worldwide.

Effective laboratory biosecurity will also depend on the bioscience community's adopting a culture that reflects an awareness of the potential misuse of biological materials and an acceptance of security practices.¹⁰ Such a transition, similar to the acceptance of laboratory biosafety several decades ago, will be important as laboratory biosecurity begins to be implemented globally.

Global laboratory biosecurity is an important step in reducing the risk posed by infectious disease and biological weapons. To achieve global laboratory biosecurity, bioscience experts worldwide must reach a consensus about the core concept of laboratory biosecurity; they must establish a template for systems that balances security and research and incorporates the unique nature of pathogens and toxins. Such a model must remain flexible in order to address the needs and concerns of specific countries and facilities while ensuring that appropriate laboratory biosecurity practices are applied worldwide.

¹⁰ Michael Moodie, "Reducing the Biological Threat: New Thinking, New Approaches," *Chemical and Biological Arms Control Institute Special Report 5*, January 2003.

2. Laboratory Biosafety and Laboratory Biosecurity

2.1 Defining Laboratory Biosecurity and Laboratory Biosafety

Before the laboratory biosecurity needs of a facility or programme can be addressed, the distinction between *biosafety* and *biosecurity* must be clearly defined.

The emergence of the term *laboratory biosecurity*, used in the context of protecting dangerous pathogens and toxins, is recent, and it is often confused with an older, more widely recognized term, *laboratory biosafety*. Laboratory biosecurity and laboratory biosafety—both critical to the operation of a modern bioscience laboratory—often overlap and should complement each other. The primary objective of both is to keep dangerous pathogens and toxins inside the laboratory; the difference lies in whether the system is designed to protect against intentional removal (laboratory biosecurity) or accidental release (laboratory biosafety).

Laboratory biosafety is a preventive measure that reduces biological risk; it aims to reduce or eliminate exposure of laboratory workers or other persons and the outside environment to potentially hazardous agents involved in bioscience or biomedical research. Laboratory biosafety is achieved by adopting a culture of responsibility among those who handle, use, and transport dangerous pathogens and toxins and through the graded implementation of laboratory *containment*, or safe methods of managing infectious materials in a laboratory setting, based on an assessment of the safety risks.¹¹

Laboratory biosecurity aims to protect pathogens, toxins, and security-related information from theft. Laboratory biosecurity is achieved by instituting a culture of responsibility, through the graded implementation of security measures that restrict access to dangerous pathogens and toxins to authorized individuals, and by establishing accountability over those materials based on an assessment of the security risks. Biosecurity, in this context, does not encompass efforts to protect crops and animals from natural outbreaks of disease or efforts to protect the food supply from contamination.

Biosafety and biosecurity must be complementary systems that function as seamlessly as possible. It should be recognized that laboratory biosecurity relies, first and foremost, on a sound laboratory biosafety programme. Yet, at the same time, good laboratory biosecurity practices reinforce and strengthen laboratory biosafety systems.

2.2 Common Components of Laboratory Biosecurity and Laboratory Biosafety

Although biosafety and biosecurity mitigate different risks, they share many common components. Good biosafety and biosecurity programmes both include risk assessment and risk

¹¹ World Health Organization, *Laboratory Biosafety Manual*, second edition (revised), 2003 (http://www.who.int/csr/resources/publications/biosafety/who_cds_csr_lyo_20034/en/). Also see National Institutes of Health and Centers for Disease Control and Prevention, *Biosafety in Microbiological and Biomedical Laboratories*, fourth edition, May 1999 (<http://bmbles.od.nih.gov/contents.htm>).

management, personnel management, material transport protocols, physical security elements, training, emergency planning, and programme management.

Both biosafety and biosecurity engage in risk management, acknowledging that risks cannot be eliminated—only mitigated. To manage risk successfully, both programmes conduct risk assessments. The results of these assessments allow facility managers to identify and prioritize risks and decide upon the appropriate levels of control.

Both programmes implement personnel measures to ensure that staff are qualified to perform their jobs, safely in the case of biosafety and securely in the case of biosecurity. The former involves verification of an individual’s technical background and skills; the latter involves understanding an individual’s character.

Both programmes should follow procedures governing the transport of biological materials. For biosafety, the shipment of infectious biological materials requires adherence to safe packaging and transport procedures, while biosecurity requires secure and accountable transport procedures.

Access control is another common element in biosafety and biosecurity. Biosafety requires laboratory access to be limited when certain types of experiments are in progress; biosecurity requires access to be limited when certain pathogens or toxins are present.

In addition, both programmes require an updated inventory of biological agents as well as emergency response plans that explain to the staff how to respond to potential safety or security incidents.

Programme management is arguably the most important tool common to both biosafety and biosecurity. The success of each of these programmes hinges on the existence of an appropriate laboratory culture that understands and accepts the rationale for the programme and the corresponding management oversight. Biosafety is reinforced through training on general biosafety practices, specific standard operating procedures, and awareness of potential safety hazards; while biosecurity training includes general biosecurity practices, specific security operating procedures, and awareness of potential security risks.

2.3 Ways That Laboratory Biosafety Contributes to Laboratory Biosecurity

In many cases, such similarities mean that existing biosafety practices, like those recommended in the World Health Organization’s *Laboratory Biosafety Manual (LBM)*, Third Edition, benefit biosecurity.

Biosafety recommendations for access controls are one such example. The *LBM* suggests that “only authorized persons should be allowed to enter the laboratory working areas.” Such access control procedures also contribute to biosecurity, which requires that the number of individuals who have access to high risk organisms be restricted.

In addition, many biosafety recommendations for decontamination, such as the autoclaving of infectious material, also contribute to biosecurity. By ensuring that biological materials and equipment are no longer harmful from a safety perspective, laboratory workers also reduce the risk that such residual material could be obtained and used maliciously to cause a deliberate epidemic.

Several recommended biosafety design features are also beneficial for biosecurity. According to the *LBM*, laboratories should have a “reliable and adequate electricity supply and emergency lighting” as well as a “stand-by generator.” By providing a continuous supply of power to laboratory areas, the facility leadership helps ensure that electrically powered physical security systems remain operational—thus reducing the risk that high risk biological agents will be vulnerable to theft. Other biosafety recommendations also support the physical security component of biosecurity. The *LBM* asserts that “strong doors, screened windows, and restricted issue of keys are compulsory,” and “other measures should be considered and applied, as appropriate, to augment security.”

The *LBM* recommends more comprehensive biosafety for Biosafety Level (BSL) 3 and BSL 4 laboratories, and many of these measures provide additional contributions to biosecurity. These high containment laboratories should be separated from areas of the building that have unrestricted traffic. BSL 3 and BSL 4 laboratory spaces may also have self-closing and interlocking anteroom doors that ensure that only one door is open at a time. The windows on these facilities should be sealed and break-resistant, and HEPA filters should be installed to provide decontamination. These laboratories should not only autoclave their infectious materials, but autoclaving must be done within the laboratory space, adding a further measure of protection. Finally, the *Code of Practice* for BSL 4 laboratories states that “The two-person rule should apply, whereby no individual ever works alone.” Such a policy contributes to biosecurity by providing a deterrent to theft.

Such contributions are heartening. Nonetheless, it must also be recognized that biosafety alone cannot provide a sufficient level of biosecurity for high risk pathogens and toxins. Additional practices must be implemented in the areas of personnel management, physical security, MCA, and transfer. In addition, a number of potential conflicts between biosafety and biosecurity must be addressed.

2.4 Potential Conflicts between Biosafety and Biosecurity

In the absence of careful implementation, aspects of biosecurity may conflict with biosafety. For example, access controls need to be implemented in a manner that does not hinder emergency response. A mechanism must be in place that allows for the emergency entry of responders but still ensures the security of the assets. Likewise, staff members must be allowed to quickly and safely exit a laboratory during an emergency, yet life safety measures must not allow an adversary to gain unauthorized access to biological materials by activating an alarm that implements emergency egress procedures.

Identification badges are often used to indicate authorized access and sometimes to enable entry, but they are not compatible with many high containment laboratories. A badge should not be

worn in situations where it constitutes a safety hazard. Badges should be required for authorized entry into buildings that contain high containment laboratories but should not be required once inside these laboratories.

Signage presents another significant conflict between the two programmes. Standard biosafety practices require that signs be posted on laboratory doors to alert people to the hazards within the lab. The biohazard signs normally include the name of the agent, specific hazards, and contact information of the investigator. Identifying the agent, its location, and the name of those individuals responsible for that agent may conflict with the objectives of biosecurity. To accommodate biosafety and biosecurity objectives, signage should be designed to disclose the hazards within the laboratory without revealing which specific agents are present.

2.5 Combined Strength of Biosafety and Biosecurity

Ultimately, to be successful, biosecurity and biosafety must be compatible, working as coordinated systems to ensure that dangerous biological assets are released neither accidentally nor deliberately.

Although biosafety and biosecurity mitigate different risks, they share a common goal: to keep dangerous pathogens and toxins safely and securely inside the areas where they are stored and used. To achieve this goal, biosafety and biosecurity utilize a number of the same programmatic components. Indeed, many existing components of biosafety contribute to biosecurity and vice versa. However, biosafety alone cannot provide sufficient biosecurity. To achieve biosecurity, new policies and procedures must be developed and potential conflicts between biosafety and biosecurity must be resolved.

3. Risk

3.1 Introduction

This section aims to support the laboratory in establishing procedures and methodologies to improve collaboration between laboratory personnel and other relevant individuals for conducting a risk assessment. Risk cannot be eliminated, only managed. Understanding the risks and the uncertainties involved is critical for management to responsibly allocate its resources. A risk assessment is the fundamental step for developing a logical and cohesive biosecurity programme that manages the identified risks through implementation of appropriate countermeasures and routine monitoring. What follows is a conceptual discussion of the components associated with laboratory risk.

Use of a risk management approach as the basis for a biosecurity programme requires assessment of the potential for (probability), and the impact of (consequence/effect), the occurrence of a particular incident. These parameters may be impossible to define quantitatively; and therefore only parametric or qualitative analysis may be available, resulting in a ranking of high to low risk across incident types.

3.2 Threat Assessment

The probability that an adversary will attack cannot be known. What happened in the past may not necessarily happen in the future. Historical data, even when available, cannot reliably predict whether or not an adversary will attack. As a result of this limitation, an adversary's *potential* for posing a threat to an asset (threat potential) may instead be evaluated by using a variety of parameters. These parameters also may not be precisely quantifiable but can be designed to address the process an adversary must undertake to identify the target and whether or not to attempt an attack. This evaluation might entail consideration of the following issues:

- Who might do this? (group or individual)
- Why? (motivation)
- With what resources or funds? (organization)
- How and when? (opportunities)
- To achieve what? (objectives)

Despite the fact that historical data cannot be used to predict the future, it does provide some context and should be used judiciously in evaluating the threat to a facility that such an event will occur again. Therefore, establishing whether there is a history of this type of attack and/or a history of activity in the area by a particular adversary is important. By evaluating all of these parameters, one can determine the adversary's threat potential.

One potential adversary is common to all facilities: the individual with legitimate access to the facility. An authorized individual who is also an adversary is known as an insider, because he or she is present inside the facility. Based on the insider as the principal adversary, biological agents may be divided into different baseline risk groups that warrant different degrees of protection against that adversary. If a facility identifies additional risk factors (as discussed in Section 3.5) that lead to the incorporation of an outside adversary into its threat spectrum, the risk may rise above the baseline level, warranting increased biosecurity measures designed specifically to address the outside adversaries with the greatest threat potential. A detailed description of each adversary class is included in Appendix G.

The setting of threat and vulnerability priorities for laboratories cannot be conducted in isolation.^{12,13} Traditionally, information on the sources of specific threats resides within security and law enforcement services. Thus, laboratories must develop collaborations with such agencies.

3.3 Consequences

For the purposes of these guidelines, consequences may be described as the potential impact of an undesired event on society and the institution.

- Population affected: An estimate of the number of people killed or who suffer serious injury or illness as a result of the undesired event.
- Economic loss: An estimate of the economic loss directly associated with the undesired event (e.g., clean-up costs from a biological terrorism event are addressed but not tourism impacts). Economic loss includes replacement costs for the asset and recovery costs.
- Functional impact: An estimate of how long it will take to recover from the specified undesired event (hours – days, days – weeks, months – years). Factors such as the existence of redundancies, backup, or contingency plans may lower the score for this parameter.
- Interdependency impact: The loss of a particular asset might have a negative impact on other assets. This relationship may be viewed as interdependent. An interdependency impact may be estimated, based on an assessment of what else could be affected and the worst-case severity of the effect(s) on those other assets (other agencies, the community, or national missions).
- Behavioural impact: An estimate of the degree to which public behaviour is affected and of the public's perception of risk. The public's perception of control over their lives or the situation may be viewed as being directly related to the availability of countermeasures (if the incident involves dangerous pathogens or toxins) and, to some degree, the facility's

¹² *On Cooperation in the European Union on Preparedness and Response to Biological and Chemical Agent Attacks* (Health Security). Communication from the Commission to the Council and the European Parliament. Brussels, 2.06.2003 COM(2003) 320 final. (http://europa.eu.int/comm/health/ph_threats/Bioterrorisme/com2003_320_en.pdf)

¹³ *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks*. United States General Accounting Office (US-GAO) 1999 Report GAO/NSAID-99-163. (<http://www.gao.gov>)

ability to communicate the facts to the public regarding the circumstances and implications of the incident.

The consequences of an undesired event will be achieved if an adversary with adequate potential (as discussed in Section 3.2) successfully executes an undesired event. An undesired event has many elements, including the asset involved, the adversary, and the objective of the adversary. For the purposes of these guidelines, the undesired event of concern is the theft of dangerous biological agents.

3.4 Baseline Risk

An assessment can determine the baseline risk posed by the biological agents held at a facility. Such an evaluation provides a means for assessing the consequences of loss of the facility's biological assets and contributes to understanding the attractiveness these assets pose to adversaries. From a biosecurity perspective, the most important assets in biological facilities are the pathogens and toxins. These agents should be protected based upon their risk of being stolen and used as biological weapons.¹⁴

The more easily an agent may be used as an effective, high consequence weapon, the more likely it is that an adversary will choose to try to acquire the agent for biological terrorism. Thus, an agent-based assessment evaluates the relative ease or difficulty involved in deploying a pathogen or toxin as an effective biological weapon, its *weaponization potential*, and its infectious disease characteristics resulting in the consequences of its use. An analysis of the weaponization potential includes such factors as the availability of a suitable strain, ease of production (an appropriate quantity in an appropriate form), modes of dissemination to achieve infection, hardiness of the agent (both in the laboratory and after deployment), and the availability and level of knowledge required to use the agent as a weapon. The potential consequences of the use of an agent depend mainly upon the agent's infectious disease characteristics. Important factors include infectious dose, incubation period, pathogenicity, availability of preventive measures and/or post-exposure treatments, and modes and ease of transmission between individuals (animals or plants) once infection occurs. By weighing both the weaponization potential of the biological agent and the consequences of its malicious use, an agent's baseline risk can be assessed.

3.4.1 Baseline Risk Levels for Pathogens and Toxins

3.4.1.1 Nonpathogenic

Nonpathogenic agents have little or no attractiveness to the adversary and are therefore not addressed in the biological asset prioritization process. No specific security measures are required.

¹⁴ Jennifer Gaudioso and Reynolds Salerno, "Biosecurity and Research: Minimizing Adverse Impacts," *Science*, 304, 30 April 2004.

Examples of agents in this exempt category may include noninfectious forms of pathogens (e.g., inactivated organisms and nucleic acids) and nonpathogenic strains.

3.4.1.2 Low Risk

Pathogens and toxins with a low baseline risk for use as biological weapons generally have low weaponization potential and low consequences. As a result, these pathogens and toxins represent a low baseline global security risk and would be considered low risk pathogens and toxins (LRPT). LRPT have a low population impact and/or inflict little economic damage. Agents with a low population impact have a limited potential to cause death and illness. Economic costs associated with the use of LRPT as weapons, would likely be low. Existing biosafety measures often provide adequate security for this risk level.

Examples of agents in this category are relatively small quantities of toxins (i.e., less than ten lethal doses for an average adult), agents transmitted primarily by parenteral or sexual exposure (e.g., malaria, hepatitis, and gonorrhea), attenuated strains, and genetic host strains of *Escherichia coli* and *Pseudomonas aeruginosa*.

3.4.1.3 Moderate Risk

Pathogens and toxins with a moderate baseline risk for use as biological weapons generally have moderate weaponization potential and moderate consequences. As a result, these pathogens and toxins represent a moderate baseline international security risk and would be considered moderate risk pathogens and toxins (MRPT). MRPT exact low to moderate casualties and/or economic damage. Agents with a low to moderate population impact have potential to cause death and illness. Economic costs associated with the use of an MRPT as a weapon would likely be significant. Existing biosafety measures, along with some additional protection measures, should provide adequate security for these pathogens and toxins.

Examples of agents in this category are plum pox potyvirus, vesicular stomatitis virus (exotic), *Coccidioides immitis*, viral hemorrhagic fever viruses, and larger quantities of toxins defined as greater than ten lethal doses for an average adult.

3.4.1.4 High Risk

Pathogens and toxins with a high baseline risk for use as biological weapons generally have high weaponization potential and moderate to high consequences. These pathogens and toxins are not particularly difficult to deploy as weapons, and their use as weapons in the maximum credible scenario could have national or international consequences. As a result, these pathogens and toxins represent a high baseline international security risk and would be considered high risk pathogens and toxins (HRPT). HRPT exact moderate to high casualties and/or economic damage. Agents with a moderate to high population impact have a potential to cause death and illness. Economic costs associated with the use of HRPT as weapons would likely be very high. Facilities with these dangerous pathogens and toxins warrant a full biosecurity programme as described in this manual.

Examples of agents in this category are *Bacillus anthracis*, *Francisella tularensis*, Ebola virus, SARS, and FMD virus.

3.4.1.5 Extreme Risk

Extreme risk agents would normally be classified as HRPT, but they receive a higher classification because they are not found in nature. As a result, these pathogens and toxins represent an extreme baseline global security risk and are considered extreme risk pathogens and toxins (ERPT). Genetically engineered agents might be ERPT if they were suspected of representing a high risk. Protection measures taken at the extreme risk level would be the most restrictive, and very few facilities are anticipated to have the need or capability to meet these security guidelines.

Currently, the only known member of this risk group is the Variola major virus, which is officially held in only two repositories. Thus, further discussion of biosecurity measures for ERPT is limited to Appendix F.

3.5 Additional Risk Factors

It is recommended that facilities consider the following questions as a starting point to further assess the risk posed to the biological materials at a facility. The additional risk factors are divided into three categories: material (i.e., the pathogens and toxins), people, and environment. Facilities will likely need to partner with local and national law enforcement and security agencies to evaluate these aspects of their environment and with security professionals to implement appropriate security measures to mitigate the impacts of these risk factors.

Material:

- How much of the material is available in the facility? In a particular laboratory?
- Has the material been modified in a way that would make it more usable as a weapon? (e.g., aerosol preparation)
- Has the material been manipulated to enhance any of the agent-based risk characteristics? (e.g., pathogenicity, infective dose)
- Are the pathogens/toxins at the facility either HRPT or ERPT, based on the agent-based risk characteristics listed above? Assumption: Beyond inherent risk that would be included in the baseline, materials of sufficiently high risk might attract an outside adversary, in which case the additional protections that address outsiders as listed below under “Environment” might be considered.

People:

Are a significant number of students or other temporary workers in the area where the material is stored or being worked on?

Do those working in the laboratory receive adequate salaries?

Do those working in the laboratory perceive their work as important and appreciated by the institution?

Environment:

- Is the laboratory a diagnostic or research laboratory?
- Does the laboratory, or do other laboratories at the facility, conduct politically sensitive work (e.g., research on animals, genetically modified organisms, or stem cells)?
- Are extremists active in the area?
- Are terrorists active in the area?
- Is the laboratory located in a high crime district?
- Is there any intelligence to indicate that the laboratory might be targeted?
- Is there a security system? If so, are any of the following features incorporated?
 - Restricted access to the materials
 - Employee and visitor screening for those who will access the materials
 - Intrusion detection system
 - Material control procedures that monitor the locations of individuals in possession of the materials
 - Information control procedures that limit access to information regarding any security measures taken to protect the materials
 - Training to address biosecurity issues

If a threat is posed by individuals who do not have legitimate access to the facility, does the facility incorporate any of the additional features below into a security system?

- Perimeter fence
- Restricted access to the building where the laboratory is housed
- Guards
- Cooperative agreement with the local law enforcement for incident response

4. Physical Security

4.1 Introduction

Physical, or engineered, security is an important component of a biosecurity system. Physical security is intended to detect and deter unauthorized access to dangerous pathogens and toxins. Physical security measures should increase as the value of the asset to an adversary increases and as the location of the asset is approached, thus forming a *graded* protection system. Determining the level of physical security for each asset may be achieved by conducting a risk assessment (as discussed in Chapter 3).

Physical security measures are intended to restrict access to dangerous pathogens and toxins to only authorized personnel. Precluding unauthorized individuals from obtaining these materials is not only a matter of controlling access into areas where these materials are used and stored, but it is also a matter of detecting breaches of physical security and then assessing these breaches to determine whether the breach was intentional or accidental. Access controls and intrusion detection systems are administered by the security officers and are supported by mechanical and automated systems. The areas being secured must also incorporate elements of delay and equivalence of structural strength, including all windows and other openings, to ensure that if an intentional breach of physical security occurs, the adversary is hindered as long as possible to afford response forces the time to arrive.

Training facility personnel on the policies and procedures associated with the physical security system is critical. Guard force personnel and/or local law enforcement personnel who may respond to physical security breaches must also be trained and must practice the activities associated with responding to a breach of security. The system must be tested and maintained on a regular basis to ensure good performance.

Physical security is supported by personnel management (as discussed in Chapter 5) and by material control, accountability, transfer, and transport procedures (as discussed in Chapter 6). The greatest degree of protection is achieved when these components are integrated and actively managed.

4.2 Graded Physical Security

Physical security should increase incrementally and form concentric layers of protection around the facility's assets. The layer within which an asset resides corresponds to the level of security it requires. In general, three layers of protection are implemented: Property Protection Areas, Limited Areas, and Exclusion Areas. (See Figure 1.) Limited Areas and Exclusion Areas are considered to be restricted areas.

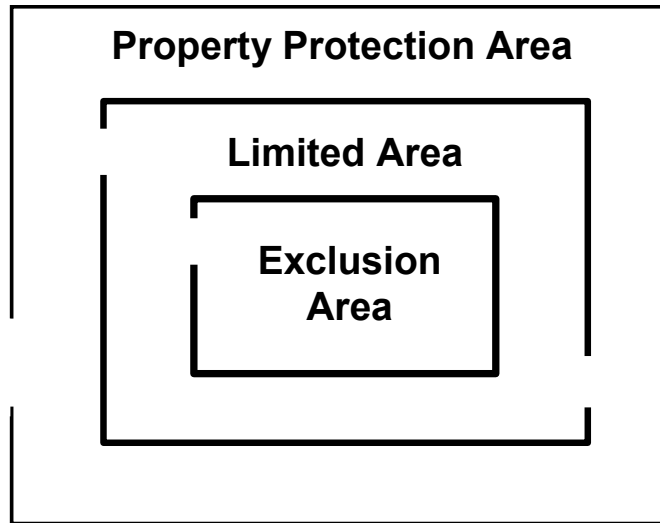


Figure 1. Graded Protection Areas

4.2.1 Property Protection Area

A Property Protection Area is defined by the outermost perimeter of a facility's campus or by the facility walls if there is no discernible exterior perimeter belonging to the facility. The Property Protection Area is intended to protect against damage, destruction, and theft of facility property. A perimeter fence may establish the Property Protection Area. Such a fence defines the boundaries of the campus as well as providing a means to control personnel and vehicle access. For facilities that hold only low or moderate risk assets, signage may provide sufficient property demarcation. A Property Protection Area can contain both Limited Areas and buildings that require little or no protection measures, such as warehouses and public access areas. LRPT may be used and stored in Property Protection Areas and may be protected to the degree provided by good biosafety practice.

4.2.2 Limited Area

A Limited Area resides within a Property Protection Area. A Limited Area has barriers that identify its boundaries and encompass the designated space. An entire building may be designated as a Limited Area, or individual rooms or laboratories that reside within a building may be designated as Limited Areas. A Limited Area has access controls and intrusion detection in place to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area. Those who are not authorized for routine access should be escorted by an authorized individual and should be required to sign a visitor log. Access to a Limited Area requires access authorization and a unique item, such as a physical or electronic key, or accompaniment by an authorized escort. Physical keys should be controlled in such a way as to ensure that they are issued only to those individuals who have a legitimate need to have unlimited access to a Limited Area and are returned when this access is no longer needed (i.e.,

upon transfer or termination). A Limited Area is appropriate for the storage and handling of MRPT as well as sensitive information (as discussed in Appendix C).

4.2.3 Exclusion Area

An Exclusion Area resides within a Limited Area. An Exclusion Area, like a Limited Area, has barriers that identify the boundaries and encompass the designated space as well as access controls and intrusion detection to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort. Access to an Exclusion Area requires access authorization and a unique item and unique knowledge, such as a physical key and positive identification provided by a guard or an electronic key and a personal identification number (PIN). Individuals who have a legitimate purpose for access, but who do not have routine access privileges, can be accompanied by an authorized escort. Both routine and visiting personnel should be required to sign an entry and exit log if electronic logging is not provided by the access control system. An Exclusion Area generally has a smaller set of individuals who are authorized to enter than a Limited Area. The keys to these areas should be controlled, and those individuals in possession of a key should be documented. An Exclusion Area is appropriate for the storage and handling of HRPT and should be used to contain animals infected with an HRPT. Sensitive information may also be stored in these areas, but a Limited Area is generally adequate. Storing information in any laboratory space presents containment issues that should be considered.

Storage containers, for instance freezers or refrigerators located within a Limited Area, when controlled with both a unique item and unique knowledge, may also be considered Exclusion Areas.

4.3 Intrusion Detection

Restricted areas should be monitored for unauthorized access. For those facilities maintaining Exclusion Areas for the storage and use of HRPT, it is recommended that security personnel monitor all entrances and exits either in person or through the use of an electronic intrusion detection system. Limited Areas do not require such rigorous controls, but personnel should remain alert to attempts at unauthorized access. If electronic access control systems are in place, alarms should be monitored and assessed.

Electronic intrusion detection systems are associated with the access control system. If forced entry occurs, or if a door or other monitored entryway is open for an extended period of time, an alarm will be generated. The electronic network should be configured to detect tampering so that if a communication line is cut or a connection box is tampered with, an alarm will be generated under this condition as well. Glass break sensors will send an alarm if a protected window is broken. Other types of sensors, including motion detection sensors and volumetric sensors, may also be used to protect Exclusion Areas and, if triggered, will alarm. All of these devices should send their alarm signals to a central monitoring station where security personnel can monitor the security system and respond to assess the alarm. The intrusion detection system

should not be connected to an open computer network. The area where the central monitoring station is located should be protected as an Exclusion Area.

Records should be kept on each actual or false (nuisance) alarm. The records should be reviewed and analysed so that corrective measures can be taken. The records should contain the date and time of the alarm, the cause of the alarm or a probable cause if a definite cause cannot be established, and the identity of the recorder or the operator on duty.

4.4 Alarm Assessment

Alarms, when generated electronically, may be assessed in person or with video. If an alarm is triggered, it should display at the central monitoring station. The individual who is monitoring this system should dispatch a response force to assess the alarm. This may be achieved by the individual leaving the monitoring station personally, in which case someone else should be in place to monitor the alarms, or by the individual calling for the support of on-site security personnel. If video cameras are integrated into the security system, they should be configured to record pre- and post-event. In other words, the images should be continuously buffered in the video camera's memory, so that if an alarm occurs, the video camera can permanently record what took place 30 seconds prior and for a number of minutes after the event. This configuration is considerably more efficient than video surveillance by humans. It also provides a means for an individual who is monitoring the security system to remotely assess an alarm to determine whether a response force is required for further investigation.

Once the alarm has been determined to be valid, someone with the capability of handling the situation in the event an intruder is still on the premises should be available to pursue the matter further. If an on-site guard force that is trained in this type of activity is dispatched to assess the alarm, they may continue as the response force. If the assessment is conducted by someone who is not equipped to handle this type of situation, that individual should summon either on-site security personnel or local law enforcement.

In a mechanically-based system, in which manual locks and guards are the main means of protection, an alarm would be generated by personal observation of an unusual situation, such as a usually locked door left ajar or a broken window. Once this situation is detected, the process should proceed with assessment and response.

4.5 Response Capability

If an alarm is assessed as valid and if the response force is not already in place, the on-site guard force or local law enforcement should be summoned. The response force should perform its duties according to a prearranged response plan. If local law enforcement is to be relied upon for this type of security incident response, a memorandum of understanding should be drawn up that details the circumstances under which the law enforcement personnel may be summoned, the protocol to follow once on-site, and the scope of authority for all parties involved. Response times should be appropriate for the protection strategy employed at the site. In other words, if the facility holds HRPT and local law enforcement cannot respond to an alarm on-site within a

reasonable period of time, the facility might consider employment of an on-site guard force. The response force should be equipped and authorized to confront an adversary.

4.5.1 On-Site Guard Force

If the risk assessment warrants an on-site response force or guard force, their role is to provide assessment and response services for any security incidents that may occur on-site. Other duties may include monitoring and responding to any alarms generated by an electronic intrusion detection system. The on-site guard force should have clear guidelines that dictate the conditions under which local law enforcement should be summoned.

4.5.2 Local Law Enforcement

Local law enforcement may be the police or other local, regional, or national security force that is trained to manage a situation in which an unauthorized entry has occurred and the adversary may be armed. Facilities that handle dangerous pathogens and toxins should ensure that all emergency response personnel, including local law enforcement, are aware of the safety issues on-site and what protocol to follow if an incident occurs.

If there is no on-site guard force, the facility should establish a clear working relationship with the local law enforcement agency to provide a response to security incidents on-site. A memorandum of understanding or a specific agreement should be established between the facility and the local law enforcement agencies. Alternatively, the local law enforcement can reinforce the on-site guard force. On-site training and orientation for the local law enforcement is also recommended.

Response force personnel should have:

- Equipment and use-of-force training
- Familiarity with facility features and operations
- Knowledge of restricted area access and biosafety issues
- Personnel cheques (See Chapter 5.)
- Specific instructions and limits of authority
- A notification list of officials who should know of the incident and the appropriate response
- Emergency response procedures
- Procedures for response to specific alarms or guard-reported conditions

4.6 Structural Issues

The perimeters that form the envelope of an Exclusion Area should, to the extent possible, be comprised of equivalently strong elements. For instance, the door should be as difficult to penetrate as the wall. Windows and other openings should be limited but when provided should be protected with either wire mesh (preferably 9-gauge stainless steel mesh fastened securely to the inside of the area) or glass break sensors. All exterior glass windows, hatches, ducts, and vents that form part of the perimeter of an Exclusion Area should be fortified to meet or exceed the strength of the surrounding wall or door.

Limited Areas should also have balanced strength of construction but do not necessarily require the level of protection required for an Exclusion Area. At a minimum all doors and windows should be closed and locked during nonbusiness hours, and the doors and locks should be robust.

Providing balanced strength around the Limited or Exclusion Area helps ensure that the most likely point of entry will be through an access controlled point.

Entry and emergency exit doors should be mounted with the hinges on the inside of the Limited or Exclusion Area, as should any hardware that is associated with securing the doors or windows, such as locks or handles. Doors to pass-through autoclaves or equipment/maintenance crawl spaces that are large enough for a human to gain access to the restricted area should also conform to these guidelines.

Panic hardware or emergency exit mechanisms on emergency doors located in Limited and Exclusion Areas should be operable only from inside the building or room and should meet all applicable life-safety codes. A local alarm that will sound when the emergency exit device is used to exit is recommended. In addition to providing immediate notification to other personnel working in the area of a possible emergency condition, a local alarm tends to discourage personnel from using the emergency exit door in nonemergency situations rather than the designated exit.

Exterior ladders should be secured to prevent unauthorized access to roofs and interior courtyards.

The overall structure of the facility and the locations of access control features are important to consider in order to ensure that the normal paths of employees and visitors enforce applicable checkpoints without providing alternate, unsecured routes and that emergency egress paths do not channel individuals into areas to which they would not normally have access.

4.7 Electronic Access Control and Intrusion Detection Systems

Modern physical security systems that include access control and monitoring are often network-based applications and, like any network-based applications, are subject to compromise. Several documented cases have shown the potential breaches to physical security by network-based attacks. To prevent these types of problems, electronic physical security systems should be managed using a separate network from the user network. The physical security system should

have no Internet access, and any required remote access should be severely limited and designed in a secure manner. Ideally an electronic physical security system would only be networked within a facility and would use only a dedicated connection when connectivity to outside networks is necessary. In addition, if an outside network connection is required, user authentication, firewalls, and encryption should be employed. See Appendix D for details on network security.

4.8 Performance Testing

Performance testing allows the effectiveness of the whole physical security system—equipment, policies, procedures, and people—to be evaluated with respect to performance. Performance testing of the physical security system should be undertaken on a regular basis in order to address any problems in equipment or procedures in a timely manner. A performance test should be based on a plan that incorporates all of the policies, procedures, and hardware components of the physical security system. The performance test plan should specify each element of the system and what test must be conducted to ensure the system is performing as intended. The plan should include testing of integrated systems of equipment and hardware, administrative procedures, and protective force procedures for both on-site guards and local law enforcement. Any change in the design or the manner in which personnel interface with the equipment will have a direct impact on the performance test plan, which should be updated accordingly.

The frequency of performance testing activities may vary depending on the type of physical security system. If the system is based largely on manpower and mechanical systems, for instance, performance testing may not need to be conducted as frequently as it would if the physical security system is electronic. In the former case, the frequency may be driven by turnover in personnel rather than the number of false alarms or routine maintenance schedules that might drive the latter. Regardless of the type of physical security system, a comprehensive performance test that addresses all physical and procedural controls should be conducted annually to demonstrate overall facility physical security system effectiveness.

Once the performance tests are complete, the results should be documented and corrective measures should be taken. Corrective measures may include replacing faulty equipment, training or retraining personnel, and amending existing policies or procedures. See also Chapter 7 “Programme Management.”

4.9 Physical Security Policies and Procedures

All personnel should receive regular training on physical security policies and procedures.

4.9.1 Policies

4.9.1.1 Access Hours

Facilities should establish normal hours of operation. All other hours are considered off-work hours, during which personal visitors should not be given access without prior approval (as explained in Chapter 5, Section 5.4.1).

4.9.1.2 Visitor Logs

A visitor to a Limited or Exclusion Area should fill out a visitor log or be logged into the area electronically. The visitor log should require information such as the names of the visitor and the escort, their signatures, the visitor's organisation, the purpose of the visit, badge number (if applicable), and the times at which the visitor entered and exited the area. A visitor log should be actively maintained for each building in chronological order for a year or more and subsequently archived.

4.9.1.3 Vehicle Security

Those facilities that have HRPT might consider implementing a vehicle control policy such that those vehicles belonging to employees and others who are authorized to have on-site parking are provided with vehicle identification tags. Security personnel should then be responsible for ensuring that only those authorized vehicles are permitted to park on-site.

4.9.1.4 Prohibited Articles

A facility may choose to prohibit certain items on the property. These items may include weapons, explosives, and other dangerous instruments or material likely to produce substantial injury or damage to property; alcohol; controlled substances, such as illegal drugs; and other items prohibited by national law. Only authorized use of video and other electronic recording devices may be required when a facility holds HRPT. Exceptions to item restrictions may be made if prior approval by the head of the facility is granted.

4.9.1.5 Consolidation

To facilitate cost-effective implementation of physical security, facilities should consolidate, to the extent possible, pathogens and toxins of similar risk levels (as discussed in Chapter 3). Such consolidation provides a means for limiting the number of areas that require restricted access.

4.9.2 Procedures

4.9.2.1 Tailgating

Tailgating, defined as more than one person passing through a controlled access point on a single key, should be prohibited. This may be a difficult provision to implement, but it is important. Often individuals feel it is a courtesy to hold a door open for another individual or, if someone knocks, to simply let the person enter. The perception is often that it is unreasonable to insist an

individual use his or her own credentials, especially if the individual desiring entrance is familiar. What must be explained to personnel is that an authorized individual can never be certain that an individual they provide access to is still in possession of authorization; this can only be ascertained by an individual's ability to obtain access using his or her own security credentials. The premise to this reasoning is that security credentials be actively managed: keys are returned upon termination or transfer, and electronic access is terminated. The exception to this principle lies in authorized escort procedures for an individual with authorized access providing access to an authorized visitor. In this case, the visitor should have documented entry and exit times, and the escort should be recorded.

4.9.2.2 Animal and Supply Handling

Care should be taken to ensure that all personnel who are responsible for the care of infected animals or who bring supplies into restricted areas are subject to the same requirements as those who have access to dangerous pathogens and toxins or that they are under escort while in these areas (as discussed in Chapter 5).

4.9.2.3 Unauthorized Individuals

Personnel who encounter an individual who cannot be identified as having authorized access, either by the absence of an identification badge, the absence of proper authorization level as indicated on an identification badge, or by unfamiliarity, should immediately report the possible intrusion to security personnel. It is not necessary that an individual who appears to be unauthorized be approached by anyone other than security personnel, but if the situation is unthreatening, the individual may be approached in an attempt to ascertain who he or she is intending to meet, who his or her escort or host is, and whether he or she is lost. If it is determined that an unauthorized individual has been left unattended by an escort or is lost, an authorized individual should escort the individual out of the restricted area and obtain assistance from security personnel. An escort who leaves a visitor in a restricted area unattended should be cited with a security violation and, at a minimum, should receive remedial training on security procedures. See Chapter 5 for details regarding escort and visitor responsibilities.

4.9.2.4 Suspicious Activity

Suspicious activity, such as in the following scenarios, should be reported to security personnel:

- An individual is observed to be displaying strange behaviour or is suspiciously out of place in the area.
- An individual is carrying a suitcase or other container in an area where this would be unusual.
- An individual is observing the facility site or operations, photographing (still or video), annotating maps, or using binoculars.
- An attempt is made to measure reaction times to physical security breaches or to penetrate physical security barriers or procedures in order to assess strengths and weaknesses.

- A vehicle is parked or operated in a suspicious manner on or in the vicinity of the facility.
- A package, suitcase, purse, backpack, or other container is abandoned in the facility or in the vicinity of the facility.
- A piece of mail has features that are uncharacteristic of routine mail, such as but not limited to:
 - External signs of tampering
 - Excessive amount of postage, no postage, or uncanceled postage
 - No return address or a fictitious return address
 - Suspicious spelling of addressee's name, title, or location
 - Unexpected mail from a suspicious address
 - Suspicious or threatening messages written on packages or contained within packages
 - Postmark showing a different location than the return address
 - Distorted handwriting or cut-and-paste lettering
 - Atypical packaging
 - Unusual, unidentified, or otherwise suspicious contents
- An individual who attempts to gain information about the facility's operations, biosecurity measures, capabilities, or personnel but does not have a legitimate need for this information should be reported. Solicitation attempts of this nature may be made by mail, fax, telephone, or in person.

4.9.2.5 Security Credential

The unique credential that provides access to a restricted area should remain in the possession or control of the individual to whom it has been assigned. The credential should not be shared with anyone, and loss or theft of the credential should be reported immediately. The credential should be returned to the institution upon termination or transfer.

4.9.2.6 Emergency Response

Personnel working with dangerous pathogens and toxins should be trained to secure the pathogens and toxins in the event of an emergency if they believe that they will not be putting themselves into jeopardy of injury. If the situation presents an imminent danger to personnel working with these materials, they should evacuate and inform security officials of the situation once it is safe to do so. Security officials should be informed of what materials were left exposed and where the exposed materials are located. Procedures to follow in the event of an

emergency should be provided to both facility personnel and emergency responders; supplemental training on these procedures is also recommended.

4.9.2.7 Other

Other procedures related to physical security, for instance the manner in which transfers are conducted, will arise during implementation of the other components of biosecurity. All procedures related to biosecurity and the consequences for failing to follow these procedures should be established and documented in the facility's biosecurity plan.

4.10 Information Security

Information security is a critical function of physical security, because the unauthorized review of physical security information could directly lead to the loss of pathogens or toxins. All physical security information warrants some level of protection. Information regarding physical security plans, user-level access, or other details of the physical security system should be considered sensitive and should be protected from unauthorized access. Facility plans, including blueprints and other details, should be considered sensitive. Electronic physical security system manuals, passwords, and other system-specific details should also be treated as sensitive.

Sensitive information should only be released to those individuals who have a direct need for the information. Protection of sensitive information should be consistent with the level of risk it poses to the potential compromise of a pathogen or toxin. The higher the level of risk associated with the pathogens and toxins the institution holds, the greater protection the information associated with the security system will require. See Appendix C for details on handling sensitive information.

This page intentionally left blank.

5. Personnel Management

5.1 Personnel Suitability

Personnel suitability refers to two components of an employee's background: the employee's qualifications and his or her personal character. Personnel should be evaluated on the basis of their technical qualifications as well as their psychological and social stability. The evaluations should be commensurate with the individual's level of responsibility. By ensuring that members of the workforce are suitable for the positions they hold, an institution can mitigate the risk of both accidental and malevolent acts.

Many biological materials cannot be accurately inventoried and cannot be detected at a distance with available technology. It is therefore possible that a knowledgeable and skilled individual with malevolent intent and authorized access could divert a microscopic amount of a dangerous pathogen from a legitimate research facility in order to perpetrate bioterrorism or to assist a prospective biological weapons proliferator. Diversion or theft of material by an insider could be accomplished without raising suspicion and is of particular concern to the biomedical and microbiological research community.¹⁵

Graded personnel suitability measures combined with access control systems and regular biosecurity and awareness training provide the best means of mitigating the insider risk.

5.2 Position Risk

Low, Moderate, or High Risk designations should be assigned to each employment position, based upon the position's level of responsibility and access to dangerous pathogens or toxins. A standard set of background investigations and/or personality tests should be developed for each risk designation group.

5.2.1 Low Risk

Individuals in Low Risk positions should have no contact with dangerous pathogens or toxins. In general, these individuals do not have duties for which mistakes, poor judgement, or an abuse of position would cause the institution significant harm. Low Risk positions often make up the majority of positions at bioscience institutions. Individuals in Low Risk positions should be allowed unescorted access to those areas where they have authorization,¹⁶ which may include Limited Areas that do not contain MRPT; but these individuals should be escorted in all Exclusion Areas and in those areas where MRPT or HRPT are present.

¹⁵ For example, see National Research Council of the National Academies, *Biotechnology Research in an Age of Terrorism: Confronting the Dual Use Dilemma* (Washington, DC: October 2003) <http://xxx.nap.edu/books/0309089778/html/>. Also see US General Accounting Office, *Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center*, GAO-03-847 (Washington, DC: September 2003).

¹⁶ Access authorization is obtained by completing all of the necessary background investigation requirements, having a need to know, and completing all required training and immunizations applicable for the areas/materials requiring access.

5.2.1.1 Job Categories

Every position that is not designated as Moderate or High Risk is by definition Low Risk. Personal and casual visitors are not given a risk designation and must be escorted in all but public areas.

5.2.2 Moderate Risk

Moderate Risk positions are those with duties that are of considerable importance to the institution, including those with significant programme or delivery-of-service responsibilities. Individuals in Moderate Risk positions should be allowed unescorted access to restricted areas where they have authorization, including those holding MRPT that they are authorized to handle; but these individuals should be escorted in all other restricted areas.¹⁷

5.2.2.1 Job Categories

Moderate Risk positions should include, but are not limited to:

- Scientists and other lab personnel with direct access to MRPT
- Shipping and receiving personnel who handle MRPT
- Personnel with investigative, law enforcement, or other security-related responsibilities other than those listed under High Risk job categories
- Laboratory support personnel who require unescorted access to areas containing MRPT. For example:
 - Safety personnel
 - Maintenance personnel
 - Housekeeping personnel
- Computer/network support personnel without root administrative access
- Unarmed security force

5.2.3 High Risk

High Risk positions are those positions with duties that have a broad scope of responsibility and authority. These duties are especially critical to the institution because of the potential consequences that could be incurred if the individual performed actions that were not in the interest of the institution. Individuals in High Risk positions should be allowed unescorted

¹⁷ Restricted areas: for example, those areas that contain MRPT, HRPT, or security-related systems or information.

access to restricted areas where they have authorization, including those areas holding HRPT that they are authorized to handle, but these individuals should be escorted in all other restricted areas.

5.2.3.1 Job Categories

High Risk positions should include, but are not limited to:

- Scientists and other lab personnel with direct access to HRPT
- Shipping and Receiving personnel who handle HRPT
- Personnel with investigative, law enforcement, or other security-related responsibilities other than those listed under High Risk job categories
- Laboratory support personnel who require unescorted access to areas containing HRPT, for example:
 - Safety personnel
 - Maintenance personnel
 - Housekeeping personnel
- Supervisors of those in Moderate or High Risk positions
- Locksmiths for restricted areas
- Computer/network personnel with root administrative access
- Personnel with administrative access to the security control system
- Armed security force

5.3 Employment Screening

5.3.1 Pre-Qualification

Prospective employees for Moderate or High Risk positions should be pre-qualified prior to being offered the position. A basic cheque of qualifications and references is generally sufficient for this purpose. Some institutions may also prefer to include a criminal cheque prior to offering an individual a Moderate or High Risk position.

5.3.2 Employment Screening

Employment screening, which may take many forms, should be conducted on all employees who hold Moderate or High Risk positions. The intent of the screening is to determine to the best of the institution's ability, based on the person's qualifications, reliability, and trustworthiness, whether a person should be authorized to have unrestricted access to MRPT or HRPT, to have unrestricted access to Exclusion Areas intended to protect information or security systems, or to hold a position of significant responsibility outside of these areas. It is a fundamental part of biosecurity to perform due diligence activities in an effort to ensure that entrusting an individual with sensitive duties is clearly consistent with the interests of the institution and international biological weapons nonproliferation.

Employment screening should be complete before granting an individual authorization to enter restricted areas without an escort. If this is not possible, the individual should remain under escort in restricted areas until such time as the screening activities are successfully completed and evaluated. Under these circumstances, the institution should reserve the right to remove the individual from the sensitive position if the results of the screening prove to be unfavorable.

The level of scrutiny an individual is subjected to should be commensurate with the level of risk associated with the position he or she will hold. Additionally, the types of screening activities may be tailored to the type of position; for instance, determining the level of an individual's financial responsibility is significantly more important for an individual holding a position with fiduciary responsibility than for a midlevel manager in charge of facility engineering activities. Criminal activity, as well as all other unfavorable information, should be carefully evaluated for the degree of the offence as well as the frequency and recency of occurrence. If a certain type of undesirable behaviour is reported repeatedly and is recent, it may weigh more heavily in the evaluation, possibly raising the issue to the level of a more serious offence.

5.3.3 Visitor Screening

Working visitors (See Section 5.4.2) should be screened in a manner that is roughly equivalent to that used to screen employees who hold positions of equivalent risk. If a working visitor is able to demonstrate to the institution that he or she has already met the requirements associated with the position at the host institution, the host institution may grant an equivalency status to the working visitor and allow unescorted access at the institution's discretion.

5.3.4 Interim Access Authorization

Interim access authorization may be granted prior to receipt and evaluation of an individual's screening data on a case-by-case basis. Some countries, such as the United States, have federal regulations that preclude granting an individual access to certain pathogens and toxins prior to completion of a U.S. Department of Justice background investigation, i.e., no interim access authorization is permitted. It is critical that each country integrate national or local regulations into their personnel management policies and procedures.

5.3.5 Screening Updates

Employees and visitors who were screened in association with their positions should have an update conducted if at any time there is reason to believe that he or she may no longer meet the standards for access. Recent arrests and negative news media reports are examples of circumstances that may motivate an institution to schedule an updated screening of an individual.

A regularly scheduled update may be warranted for persons holding higher risk positions. Generally every five or ten years is sufficient.

5.3.6 Derogatory Information

Derogatory information is unfavorable information regarding an individual that brings into question the individual's eligibility or continued eligibility for unescorted access authorization to restricted areas or materials.

A sample scheme for categorizing criminal offences is presented below:

MAJOR ISSUES:

- Any terrorism issue

SUBSTANTIAL ISSUES:

- Undesirable patterns of conduct, including alcoholism or drug addiction, financial irresponsibility or major liabilities, dishonesty, lack of employability for negligence, misconduct, or criminal conduct
- Drug manufacturing, trafficking, or sale
- Major honesty issue, such as extortion, embezzlement, or perjury
- Serious violent behaviour, such as rape, aggravated assault, arson, child abuse, or manslaughter
- Illegal use of firearms or explosives
- Employment-related misconduct involving dishonesty or criminal or violent behaviour

MODERATE ISSUES:

- Driving while intoxicated
- Drug-related offences (other than those listed above)
- Theft or forgery

- Disorderly conduct, assault, criminal mischief, or harassment
- Employment-related misconduct involving insubordination, absenteeism, or rules violations

Criminal offences are just one form of information that may surface in the process of screening an individual for employment. Other forms of data should be categorized in a similar fashion to provide a framework for evaluation.

The manner in which issues that arise through employment screening are evaluated should entail reviewing both the seriousness of the offence and the timeline in which it occurred. A single offence of significant consequence may warrant a decision not to hire an individual or to remove an individual from certain duties. A lesser offence might warrant an interview that provides the individual with an opportunity to explain the circumstances under which the offence occurred, possibly providing the institution with the satisfaction that the individual is suitable for the position despite the recorded offence. A pattern of lesser offences may warrant actions that would only be taken in response to a more serious offence, if there is no demonstration that the pattern has been broken. The institution should have a documented rationale for how the information gathered in a pre- or postemployment screening will be evaluated and used. All screening results and evaluations should be treated as sensitive information

It is the responsibility of each individual holding a Moderate or High Risk Position to report to his/her management any derogatory information that may impact the status of his or her access authorization.

5.4 Visitor Control

The term *visitor* in this context includes any person, employee or otherwise, who does not have access to a restricted area but who has permission to enter and is therefore provided access with an authorized escort. Visits to restricted areas should be prearranged, and a visitor should display an appropriate badge. Visits to restricted areas should be limited to official business.

5.4.1 Personal Visitors

Personal visitors, including personal friends, relatives, spouses, and children, should only be permitted in unrestricted areas during normal business hours, and such visitors should remain in the company of their hosts.

5.4.2 Working Visitors

Working visitors may fit into various categories, including any individual who is not employed by the institution but who has official business to conduct on the premises. If a working visitor is anticipated to be on-site for more than 30 days or if the working visitor requires unescorted access to restricted areas, it is recommended that the visitor be screened in the same manner as

an employee. The screening activities should be conducted as soon as the visitor arrives or in advance of his or her arrival in order to avoid the impact of long-term escorting.

Providing an escort into restricted areas is recommended for those individuals, such as maintenance staff, who require regular access to restricted areas but who do not require access to dangerous pathogens or toxins.

5.4.3 Limited Areas

A visitor to a Limited Area should remain under escort unless the visitor has met the requirements for unescorted access.

Couriers and other delivery personnel should either deliver their packages to an area where they do not require an escort, leave the delivery with a guard, hold authorized access, or be escorted.

5.4.4 Exclusion Areas

Casual visits to Exclusion Areas are discouraged; however, guided tours and other demonstration-related activities are occasionally necessary. Under these circumstances, great care should be taken to secure all dangerous pathogen sources and to keep each visitor under escort at all times.

Those individuals who are not employed by the institution but who have been invited to work in an Exclusion Area should meet the same criteria as employees of the institution who have unescorted access to the Exclusion Area. These criteria should preferably be met prior to the individual's commencement of work in an Exclusion Area, but if this is not possible, the individual should remain under escort until such time as unescorted access may be granted.

5.4.5 Unescorted Visitor Access

A working visitor to a restricted area who has met or exceeded the requirements the institution imposes on its own employees may submit information that demonstrates this fact in advance of his or her arrival and request unescorted access to the appropriate restricted area. The visitor should only be granted unescorted access to the specific areas where he or she will be working. Upon granting access, the institution should provide the visitor with a badge that illustrates the visitor's status and with the keys required to access the approved areas.

5.4.6 Host Responsibilities

Each visitor should have a host at the institution who is responsible for ensuring that all the appropriate members of the institution staff who will have some responsibility associated with the visit are informed of the visitor's arrival and duration of stay. The host is also responsible for ensuring that the visitor is properly escorted and is provided with an appropriate badge.

5.4.7 Escorting

Individuals who have a need to know and permission to enter but who have not been cleared for unescorted access must be escorted in restricted areas. This includes visitors; support personnel who are required to enter the area for maintenance, repairs, or cleaning but who are not cleared for access; as well as all other individuals without the appropriate institutional identification and keys that would provide them access to a given area.

Escorting should follow a variety of conventions:

- Within a Limited Area, the visitor-to-escort ratio should not exceed 8-to-1. Within an Exclusion Area, the visitor-to-escort ratio should not exceed 1-to-1 for working visitors and 4-to-1 for tours or other demonstration-related activities.
- Within a Limited Area, administrative escorting procedures should be allowed, i.e., an individual under escort may go to the lavatory or get something to drink on the same floor without the escort in attendance. The escort must know where the individual is, and the individual must understand that he or she is not permitted to conduct any other than the prearranged activities and should return to the escort promptly.
- The escort should have authorized access to the areas being visited.
- The escort should remain with a visitor and maintain verbal and visual contact at all times while inside an Exclusion Area.
- The escort should be knowledgeable about the area in which the visitor will be escorted.
- The escort should inform the visitor of articles that are prohibited on the premises and of any restricted area prohibitions.
- The escort should ensure that visitor logs are completed where applicable.
- The escort should ensure that a visitor wears his or her badge above the waist in plain view.
- If control of a visitor is turned over to another authorized escort, the original escort should ensure that the new escort is aware of the escort responsibilities.
- The escort should notify security personnel who may monitor the site after hours if the visitor and the escort intend to remain in a restricted area beyond normal working hours.
- The escort should ensure that the visitor's badge is returned at the end of each workday or upon expiration.

If an unthreatening, unauthorized individual is found unattended in a restricted area, an explanation of who is escorting the individual and why the escort is not present should be obtained. The individual should be escorted from the area and delivered either to the host (or host organisation) or to a security guard if security guards are present on-site. At no time

following discovery should an unauthorized individual be left unattended in a restricted area. If an individual or situation appears to be dangerous, someone responsible for responding to security incidents should be called immediately. Any occurrence of suspected or confirmed unauthorized entry should be reported to the organisation or individual who is responsible for the institution's security immediately.

5.5 Badges

Every individual at a bioscience institution that has dangerous pathogens and toxins should wear a badge. Preferably, such badges will be designed to be difficult to replicate, will include a photograph of the employee, and will possibly have an electronic access mechanism to allow the badge to also act as a key. Each visitor should also be issued a badge. A visitor's badge may or may not include a picture; but if the visitor is a working visitor, a picture badge similar to those issued to employees but with an indication that it is a visitor's badge, is preferable.

A badge should be worn on the institution's property except in areas or situations in which the badge might compromise safety. In facilities where the badge provides a means of gaining access through electronically locked doors, another means of access control, such as a keypad for PIN entry or a biometric device, should be employed in areas where wearing a badge would present a safety hazard.

The badge should be worn above the waist with the photograph in full view. The institution's badge should not be used for unofficial identification. Any time an individual's appearance changes significantly, a new photograph should be taken and a new badge issued. Employee badges should expire every five years. Visitor badges should expire upon termination of the visit or every five years, whichever comes first. Upon expiration of his or her badge, the employee or visitor with a continuing engagement at the institution should get a new photograph and a new badge.

Badges with electronic access mechanisms should be encoded to allow individuals access only to those restricted areas that they are authorized to enter. Authorization should be contingent upon meeting the suitability requirements of the position, need to know, completed biosafety and biosecurity training, and being current on any applicable immunizations. An individual's access authorization should be updated if any of these factors change or if his or her compliance lapses. Ideally, an electronic notification system would be in place to facilitate management of these compliance-related factors.

Employee badges should include:

- An institution identifier
- The individual's photograph
- The individual's name
- The expiration date, visible and/or encoded if badge contains electronic access control capability

Other badge features could include:

- Restricted area colour coding or symbology
- Indication of whether the individual is authorized to access animal areas
- Indication of whether the individual is an emergency responder

Entering a restricted area without a proper badge and access authorization should constitute a security infraction. Anyone with access authorization is responsible for ensuring that individuals who have lost access authorization or who are unauthorized are not permitted entry into restricted areas. Unauthorized individuals may be recognized by the absence of a badge. An individual who forgets his or her badge is responsible for obtaining a replacement.

5.6 Employee Assistance Programmes

Institutions that have biosecurity programmes should provide employees with a mechanism to address personal problems. Personal problems left unaddressed may deteriorate into situations that present security concerns, and proactive management in these situations is highly recommended.

The institution should establish an employee assistance programme (EAP) that provides sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

The objectives of the EAP may include:

- Ensuring employees can perform their jobs in a reliable and safe manner
- Providing early diagnosis, treatment, and rehabilitation referrals and/or resources for employees requiring medical attention for mental health or substance abuse problems
- Applying preventive measures towards maintenance of mental and physical health through health promotion and education
- Providing resources intended to facilitate resolution of problems associated with:

- Marital issues
- Family issues
- Eldercare/childcare issues
- Job conflict
- Grief
- Financial issues
- Legal issues
- Stress

5.7 In-Processing

Every employee or visitor who requires access to a restricted area should complete all required personality test/background investigation forms, biosafety training, biosecurity training, and immunizations as applicable to the assigned work environment prior to issuance of any keys.

It is also important to ensure that each individual receives a security briefing prior to receiving a badge in order to ensure that the individual is aware of the institution's security and safety policies and procedures. The briefing should consist of a selection of training modules. Modules should be available for: host/escort requirements, challenging unauthorized individuals, badging requirements, computer security, and safety.

5.8 Out-Processing

Out-processing should be conducted when an individual leaves a position, whether the individual is leaving the institution or changing positions.

5.8.1 Access Changes

Changes in access may result from changes in job classification or job location. These changes should be reflected in an individual's access authorizations. Any mechanical keys that are no longer required should be returned. Any combination lock that is no longer needed by the individual should have its combination changed if it is located in an Exclusion Area and possibly if it is located in a Limited Area, depending on the criticality of the asset being secured. Any information system access that is no longer necessary should be removed and new authorizations for additional access implemented.

5.8.2 Termination of Access

An individual who is planning to be absent for any length of time should be expected, in a timely manner, to notify his or her supervisor, secretary, office mate, or other responsible individual who can ensure that others who need to be aware of the individual's absence are informed. Any unexplained absence of a significant period of time, to be established by each institution, should result in termination of any electronic access.

Routine termination procedures should ensure that computer passwords and any other electronic means of physical or electronic access are deleted/terminated upon an individual's date of termination. An exit interview between the individual and his or her supervisor is recommended. The interview should specifically include a discussion about continuing security responsibilities regarding any sensitive information gained while working at the institution. The individual's final paycheck should be withheld until such time as all of the institution's property, such as badges, keys, and computers, is returned.

More specifically, items that should be returned and information that should be obtained from the outgoing individual may include:

- Identification badge, electronic keys, smart cards, and any other means of electronic access (Electronic access should be terminated immediately.)
- Portable vehicle passes (Individuals should be encouraged to scrape off any permanent vehicle pass upon out-processing.)
- Mechanical keys
- Identification of combination locks requiring new combinations
- Sensitive documents and drawings, both electronic and hard copies
- Work records/files, both electronic and hard copies
- Laboratory notebooks
- Identification of all dangerous pathogen sources that the individual was working with that have not been destroyed, e.g., samples, working stocks, animals
- Computer software and hardware disposition (portables returned, office equipment reassigned)
- Telephone disposition (portables returned, office equipment reassigned)
- Computer password(s) (canceled)
- List of network and computer system accounts

- Pagers
- PDA (personal data assistant)
- Library materials
- Signed nondisclosure agreement for those individuals who are knowledgeable of proprietary or security-related information

5.9 Counterintelligence Awareness Training

All employees and long-term working visitors should receive general counterintelligence awareness training once a year. This training should assist lab members in identifying situations or actions by persons outside the laboratory who may indicate an intention to obtain information or materials from within the laboratory without authorization.

All individuals in Moderate and High Risk positions should be encouraged to take additional, role-specific, counterintelligence awareness training. Training should address information specific to the various positions, such as:

- Positions with access to dangerous pathogens and toxins
- Positions with access to proprietary information that may be vulnerable to corporate espionage
- Computer system administrators
- Positions with high degrees of corporate fiscal responsibility
- Security force personnel

Individuals who hold positions in each of these areas have access to different institutional assets that may be targeted for acquisition by an outsider. The type of adversary and the methods used will vary depending on what the adversary is interested in obtaining. The training should therefore be specific to the asset that may be targeted. Individuals in Moderate and High Risk positions should be trained to identify and avoid situations that may put the institution's assets in jeopardy and to report to their managers or institutional security officials any attempt by an outsider to inappropriately solicit information or materials from the institution.

5.10 Security Infractions

The term *security infraction* is used to indicate that an individual has broken a security policy. Once an institution's management is notified of an infraction, the employee should be counseled and reminded of the policy that was violated. The penalty for security infractions should vary depending on the offence. Penalties for lesser offences might include a note in the individual's

security file, removal of access privileges, and/or disciplinary action, while greater offences may warrant termination and possibly criminal prosecution. Multiple minor incidents should elevate the response to subsequent incidents.

Security policy infractions should include:

- Leaving an individual who requires escort unattended in a restricted area
- Following an individual through an electronically controlled access point without providing individual access-granting credentials, such as a cardkey (This does not apply to situations where a visitor is under escort but includes both normally authorized individuals entering restricted areas without a badge, when not precluded for safety reasons, and unauthorized individuals following an authorized individual through an access control point. This infraction is allocated to the individual who does not provide the credential.)
- Providing access into a restricted area for an unauthorized individual (This includes opening the door for the unauthorized individual; providing the unauthorized individual with a key, a combination, a cardkey, a password, a PIN, or any other means of entry; as well as propping open an access controlled door and leaving it unattended. This infraction is allocated to the individual who provides access.)
- Providing access to computer information systems at an unauthorized level (This includes leaving a computer unattended while logged into a restricted network or while accessing restricted information without a password-protected screen saver engaged or providing other unauthorized personnel with a password or other means of access.)
- Bringing a prohibited item, e.g., a firearm or illegal drugs, into a restricted area
- Giving false identification to, or failing to follow instructions from, a security force officer
- Removing dangerous pathogens or toxins or sensitive information from the area of their storage or use without proper authorization
- Discussing sensitive information with an unauthorized individual (Any presentation that has not gone through a review and approval process and is found to contain sensitive information following dissemination to unauthorized individuals should result in the author receiving a security infraction.)
- Failure to report derogatory information to management in a timely manner
- Failure of management to provide leadership in a situation that results in a security event, regardless of whether harm occurred
- Knowing falsification of, destruction of, concealment of, omission of, or tampering with evidence or data relative to a security event

- Unknowing (minor) or knowing (major) violation of security business rules that may reasonably be expected to result in the compromise of protected materials (Unknowing violations may constitute a pattern of disregard or lack of attention that could lead to security breaches.)
- Intentional conduct that has a high probability of resulting in compromise of protected materials or acts for which criminal penalties could be imposed (Examples include selling or stealing dangerous pathogens or toxins and theft of the institution's property.)

5.11 Information Security

Information security as a function of personnel management is needed to ensure that human resource information, specifically personal information, is not inappropriately released to the public or to anyone without a direct need for such information. Beyond being an employee confidentiality concern, personal information can be a biosecurity concern, as it can allow the targeting of persons with access to dangerous pathogens or toxins. Background and personality test results could also be used in an inappropriate manner or could be used to coerce or embarrass a person with access to pathogens or toxins. Information of this type should be controlled as sensitive information. (See discussion in Appendix C.) Additionally, any information or data that is associated with an individual's level of access to dangerous pathogens or toxins and that is stored in a personnel system should be considered sensitive. Compromise of these systems can directly lead to loss of a pathogen or toxin.

Any persons with root administrative access to personnel information should be aware of the information sensitivity levels and cognizant of any actions taken in the handling and protection of personal information. Additional training and policy controls may be needed for individuals with access. Personnel information should be marked, stored, and transmitted within the guidance established for the level of sensitivity associated with this form of information. Any electronically stored personnel information should be protected within the computer and network security guidance established for information of this sensitivity. Only those individuals with a need to know should have access to any sensitive personnel information, whether it is recorded in a paper, electronic, or other format. Those individuals with access to sensitive personnel information are themselves within a Moderate or High Risk position, depending on the level of access.

This page intentionally left blank.

6. Material Control and Accountability

6.1 Introduction

Material control and accountability is a necessary component of a comprehensive biosecurity programme. It complements other measures, such as providing physical security, granting access only to trusted individuals, and protecting sensitive information, to name just a few. Alone, MCA would not be sufficient to implement biosecurity. Biosecurity without MCA would likewise be inadequate.

In MCA, *material* refers to pathogens and/or toxins and anything containing them, subject to certain exclusions detailed later. *Control* is the combination of engineered and procedural measures that ensure materials are used only as intended and not diverted for malicious or unknown use. *Accountability* ensures that these materials are controlled as intended, by formally associating the specified materials with the people who provide oversight. Together, MCA provides the timely knowledge of *what* materials exist, *where* they are, and *who* is accountable for them.

Because the material is biological, applying quantitative material balance accounting is not feasible, particularly in dealing with bulk material. For replicating material, any quantity is significant, because often only a single organism is needed to create a virtually unlimited population. To some extent, measures can be taken to *contain* materials so that some accounting of containers that hold these materials (as *items*) may be possible, especially for long-term storage of repository stocks. Otherwise, the use of accounting as a tool to detect the diversion of material is not realistic. Instead, for biosecurity, trusted individuals are ultimately relied upon to provide active oversight; thus the term *accountability* rather than accountancy.

MCA also involves material transfer within a facility, between facilities within a country, or internationally. Scientists, health agencies, and diagnostic laboratories rely on the timely exchange of biological materials for a variety of reasons. During transfer, materials outside a restricted area are more vulnerable to theft or tampering. Accountability of the material, documentation, and oversight during the transport process are measures that improve biosecurity.

As with other components of biosecurity, MCA measures are *graded*. Those materials of the greatest biosecurity concern are subject to the most stringent MCA measures, while those of lesser concern are subject to correspondingly lower MCA effort. The material classifications of LRPT, MRPT, HRPT, and ERPT, as described in Chapter 3, correspond to graded MCA measures, which become more robust as the risk of the material increases. The rationale for the graded application of MCA measures is simply to allocate resources sensibly and effectively. By their nature, MCA measures involve additional cost in time and effort; and it is prudent to minimize such intrusiveness whenever possible.

The issues for MCA involve defining precisely:

- What materials are subject to MCA measures
- How control is exercised for those materials
- How accountability is implemented and what it entails

Furthermore, consideration must be given to:

- Timeliness requirements for MCA information
- Archival or historical requirements for the information
- Reporting requirements
- Audit requirements
- The information security implications of MCA information
- Continuity of MCA through the complete life cycle of subject materials—their creation, storage, use, movement, and disposal

The information that results from the implementation of MCA practices is itself a concern for biosecurity. Dissemination of that information needs to be governed on a need-to-know basis that ensures good accountability yet does not itself impair biosecurity by providing valuable information to would-be adversaries. While detailed information about pathogen inventories may need to exist at a laboratory level for example, only an abstracted, aggregated summary of that information may need to be distributed more broadly.

6.2 Materials

Any container, organism, culture, sample, or other object known to contain any dangerous pathogen or toxin is subject to MCA measures. Unknowns should be added to the inventory, and an accountable scientist should be assigned as soon as diagnosis confirms the presence of a dangerous pathogen or toxin. Dangerous pathogens and toxins exist in many different forms and containers, depending on the method of storage, but may be divided into two general categories for the purposes of MCA.

Hereafter, reference to *materials* is meant to imply *those materials subject to MCA measures*, unless specifically indicated otherwise.

6.2.1 Agent

Materials are those indicated on a list of agents that are deemed to meet the criteria for LRPT, MRPT, HRPT, or ERPT, as determined by national, regional, local, or facility authority. (See Appendix F for ERPT MCA procedures.) The defining list of materials can change, especially

because new agents and strains are likely to appear, so MCA measures need to be prepared to respond accordingly.

6.2.2 Quantity

The quantity of replicating organisms is not meaningful: any amount is considered significant.

The quantity of toxins and other nonreplicating materials is meaningful, however. Any amount should be subject to MCA measures unless it can be shown that the total quantity for the particular laboratory or institution is less than the regulatory or policy-based threshold for the material in question.

6.2.3 Form

Pathogens and toxins exist in a wide variety of forms. For example, they may be present in liquid solution in a laboratory container, may be infecting a biological organism, may be contaminating equipment or filters, or may exist as spores that are easily airborne.

Whenever possible for MCA purposes, material should be aggregated into *items*, i.e., discrete, identifiable, and countable units. Each item can then correspond one-to-one with an associated information record that is required as part of accountability. Although the associated quantity of material within the item can be specified, it is essentially irrelevant for MCA.

All items should be labeled so that the contents can be readily identified and so that their association with MCA information records is clear.

Repository Stock Cultures

Repository stock cultures of MRPT or HRPT materials should be maintained in storage vaults or freezers within restricted areas. Such cultures are the source material for working samples.

Working Samples

Working samples of MRPT or HRPT are those materials that are currently in use for culturing, analysis, or other laboratory experiments and should also be located in restricted areas. In most cases, corresponding repository stock cultures exist for all working samples. Exceptions include studies that introduce mutations into a line to determine which is best for a certain research or diagnostic purpose. After identification of the desired sample, mutations that are not selected should be destroyed and the new mutation documented using MCA procedures.

Unknowns

Samples of unknown content do not need to be subject to MCA. If a sample is suspected of containing materials subject to MCA procedures, it is certainly appropriate to apply MCA measures, provided the uncertain status is noted. Once a sample has been positively identified as MRPT or HRPT, it should be subject to MCA measures.

Clinical Samples

Materials may originate from clinical work outside a laboratory. Clinical samples shipped to and received by a laboratory for diagnosis or other analysis should be subject to special handling, because they are not yet captured by MCA measures. Once confirmed to contain controlled materials, however, a sample and all its derivatives should be subject to the associated control and accountability measures, even if it is ultimately destroyed.

Genomic DNA, plasmid DNA, and RNA

All forms of DNA and RNA that contain known genes associated with a dangerous pathogen or toxin should be subject to the same MCA measures as would be applied for the material itself. WHO guidelines regarding the biosecurity of DNA should be followed. For example, the WHO mandates that only 20 percent of the Variola major genome may be present at any one time in any laboratory that is not a WHO-recognized smallpox repository. It is appropriate to apply MCA measures for genomic libraries of dangerous pathogens and to keep accurate inventory of identified genes from an organism.

Contamination

MCA does not apply to equipment, instruments, clothing, and similar laboratory objects that have been, or may have been, contaminated with materials. Such contamination should be cleaned up promptly and disposed of properly in an appropriate area¹⁸ to assure that no trace of pathogen or toxin remains. MCA should already have captured those materials that could have been the source of the contamination.

6.2.4 Detail

MCA measures may differ in the level of detail required. For example, for LRPT, merely indicating that the material exists in a particular laboratory or a particular freezer may be sufficient and otherwise may not require more detail. On the other hand, HRPT would need to be more tightly controlled, and individual vials would need to be tracked separately.

6.2.5 Required Information

For MCA purposes, certain information about materials must be provided. The information falls into three categories:

- **Attributes:** information needed to characterize the material, i.e., to describe *what* it is. This category includes the agent/strain information and possibly its origin, its date of origin, its source history, the quantity, various measured data, etc.

¹⁸ Autoclaves and other forms of decontamination equipment used for MRPT and HRPT materials should reside within the restricted area that is used for laboratory and storage purposes.

- Description: information needed to identify *which* item it is. Especially when multiple items exist, it is important to specify the container, its identification, its location, etc.
- Type or classification: used to designate the biosecurity significance of the item, whether it is classed as LRPT, MRPT, or HRPT.

Other information associated with materials, such as the scientific or medical application of interest, could also be kept with the MCA-required information. It is useful to have a ready means to separate the MCA-relevant and technical information so as not to compromise biosecurity or intellectual property concerns by unnecessarily disclosing information.

6.3 Control Measures

Control is implemented to ensure that materials stay or, in the case of legitimate transport, go where intended and that they are used for a stated purpose by appropriate, authorized people. Control measures include ensuring that sensitive information is marked and handled correctly. Control can be accomplished in one of two ways. Engineered, or physical, control is a means of preventing unauthorized access, such as locking a freezer, strengthening network security systems, or using an interlock on an autoclave that prompts a user to specify contents before running, and requires a log be kept of all operations. Otherwise control is accomplished through operational procedures. Existing procedures may not be relevant to biosecurity, so all existing procedures should be reviewed and updated to incorporate biosecurity measures. New procedures specific to biosecurity may also need to be developed. Ideally, biosecurity would be integrated with the overall laboratory procedures that exist for other reasons, such as biosafety. Both biosecurity and biosafety procedures should be documented.

Control should be effective under both normal and abnormal conditions. Material storage, use, and typical changes (such as creation, modification, or destruction) are normal conditions. Abnormal conditions, such as inventory discrepancies (something appears to be missing), anomalies (something does not look right—e.g., a freezer left unlocked), or accidents, also require procedural responses.

The following section lists certain minimum objectives for control measures, which could use either engineered controls or operating procedures or a combination of controls and procedures to accomplish the desired objectives.

6.3.1 Confine Materials to Restricted Areas

Materials should be stored and used within restricted areas and in a manner consistent with the WHO biosafety standards. Such areas limit access to authorized individuals only. (See Chapter 4 “Physical Security” for a complete description of restricted areas.) The facility and laboratory inventories should identify where pathogens and toxins are located.

The only materials permitted outside a restricted area are those that are being shipped or transferred from one location to another. These materials are then subject to the policies and

procedures for material transfer that should include provisions for maintaining chain-of-custody and international transport standards. WHO has provided guidelines for the safe transport of infectious substances and diagnostic specimens.

6.3.2 Material Identification

For inventory purposes, materials should include enough information for a knowledgeable person to identify the material readily. This might include information such as strain, sample type, and concentration. The system must be detailed enough to allow the material to be identified accurately.

6.3.3 Material Disposition

Procedures should be in place at each location to inactivate and dispose of materials. The dates and methods of disposition of materials should be recorded in the inventory and the record retained for historical archive.

6.3.4 Physical Inventory Taking

A physical inventory is accomplished by identifying and listing all materials item-by-item in a particular area, such as a laboratory or a workstation within a laboratory. The physical inventory taking (PIT) is assembled by a thorough search and review of all locations where the materials may exist. A PIT should be conducted periodically, with the frequency depending on the material category.

The information record obtained from the PIT then becomes what is called the *book inventory*. Thereafter, the book inventory is maintained by recording changes that take place after the PIT, e.g., materials produced, transferred, consumed, or destroyed. The information can be kept by manual ledger, such as in a designated notebook, or as an electronic database.

Whenever a PIT is conducted, the physical inventory should be compared with the current book inventory to identify any discrepancies. Any discrepancies indicating theft or unexplained loss of materials should be reported immediately to the accountable scientist and, if appropriate, local and national authorities.

Various measures may be involved in a PIT, including identifying items, counting items, and making diagnostic measurements to verify contents. When large numbers of items are involved, especially for lower-risk materials, selective (statistical) sampling for identification or diagnosis may be employed.

6.4 Accountability

It is not sufficient to identify and control the materials. Accountability is the means of ensuring that materials are properly secure. Assigning qualified oversight for all materials, keeping

records, reporting, and auditing are all aspects of accountability. A person with expert knowledge of a specific controlled biological material, its use, and its storage should be named as a point of contact for the material. When pathogens and toxins are transferred, the legitimacy of the carriers and of the receiving facility should be verified.

6.4.1 Accountable Scientist

Each dangerous pathogen and toxin should have a designated accountable scientist who is knowledgeable about the assigned pathogen or toxin in storage and in use. The accountable scientist is responsible for providing information about how, when, where, and why his or her assigned pathogens and toxins have been used, transferred, or destroyed and is responsible for maintaining current accountability records. Accountable scientists are responsible for overseeing the work associated with their assigned pathogens or toxins. Any anomalies should be reported to the appropriate officials promptly.

The head of the facility should be responsible for ensuring that an appropriate accountable scientist has been assigned to each dangerous pathogen or toxin located in the facility.

6.4.2 MCA Records

Information records are part of the accountability aspect of MCA. It is important that they be accurate, complete, and timely. MCA information might prove useful to an adversary, so it should be treated as sensitive information and should be subject to information security practices. MCA information often overlaps with information recorded for scientific purposes, so care should be taken to prevent sensitive MCA information from inadvertently being released to the public. (See Appendix C.)

Accountability records are sensitive information and are subject to the policies and procedures for restricted information. Accountability records should be kept at laboratory and facility levels and at a national level, if appropriate. Information in each system should be consistent.

Laboratory Notebooks

Laboratory notebooks should be required for LRPT, MRPT, and HRPT.

All activity involving LRPT, MRPT, and HRPT materials should be recorded in laboratory notebooks. Information should specify what experiments were performed, by whom, and when. Active laboratory notebooks associated with MRPT and HRPT materials should not be removed from the restricted area when filled; laboratory notebooks need to be maintained as archive records. These records may need to be stored in a secure location, depending upon concern about the materials documented in the laboratory notebook.

Facility Inventory of Repository Materials

Each facility that stores or uses MRPT or HRPT materials should maintain a detailed inventory in a secure, limited-access electronic database. The inventory should include all dangerous

pathogens and toxins at the facility. The inventory covers all repository stocks as well as any dangerous pathogen or toxin that might not exist as an isolate in a repository stock culture. The facility inventory should include information about the location of each of the dangerous pathogens and toxins and its associated accountable scientist. Accountable scientists for dangerous pathogens and toxins are responsible for entering inventory data and for keeping all records up to date.

National Pathogen and Toxin Inventory

In some cases, it may be appropriate to consider submitting inventories to a national registry. Laboratories, through their respective agencies, provide the information for that database on a timely basis. Summary records consolidated and abstracted from the facility inventories of MRPT or HRPT should be transmitted electronically via secure and authenticated channels and stored in a secure, limited-access electronic database. Ideally, the national database should be kept up to date automatically using electronic conduits or scripts, which would relieve the agencies and laboratories of manual reporting while ensuring the timeliness, consistency, and security of the information. A national database would enable governments and managers to determine rapidly what dangerous pathogens and toxins are or have been in use at each facility and how to get additional information if needed. The registry should include the following information:

- Agent name
- Agency/location/laboratory
- Person responsible for pathogenic material (laboratory supervisor)
- Contact information
- Date of disposition

Except for working stocks, all dangerous pathogens and toxins should be included in the inventory system. New dangerous pathogens and toxins, identified in diagnostic experimental samples or generated through recombinant technologies, should be added to the repository and inventory.

6.4.3 Timeliness and Historical Archive

Inventory of materials should be kept current by recording any changes to the inventory at least daily. Historical records should be kept for all dangerous pathogens and toxins for at least five years after the date of final disposition.

6.5 Low, Moderate, and High Risk Pathogens and Toxins

6.5.1 LRPT

A laboratory notebook maintained by the accountable scientist should document the stocks and the use of materials. Laboratory management should keep a record of where LRPT materials are stored and used and a record of who are the accountable scientists.

The transport of LRPT should also be documented in the laboratory notebook. Recorded information should specify what was shipped and should include the date and destination of the shipment, the name of the person expected to receive the shipment, the name of the carrier used to ship the material, and the tracking information for the shipment.

6.5.2 MRPT

MCA measures for MRPT materials are based on those for LRPT, such as maintaining information in laboratory notebooks, but should include additional measures. Inventories should be maintained in secure, limited-access databases that are consistent throughout the facility.

Information about the transfer of MRPT should be included in the laboratory inventory database. Paper documentation of the transfer, such as carrier receipts, should be kept for historical documentation of the transfer. If temporary storage needs to be provided for packages awaiting transit, the security should be equivalent to that for the Limited Areas used for handling MRPT. The accountable scientist responsible for shipping the materials should have knowledge of the professional nature of the receiving laboratory and should know that the individual receiving the material is qualified to work with MRPT.

6.5.3 HRPT

All MCA measures for HRPT are based on those for MRPT, with the following additional guidelines:

Transfer should be authorized and approved by the facility's biosafety officer or other designated responsible official before the material ships. The designated responsible official for the sending laboratory should confirm that both the receiving laboratory and the receiving individual are qualified to accept HRPT materials.

If temporary storage needs to be provided while packages are being held in shipping and receiving areas or during transit, the security should be equivalent to that for the Exclusion Areas used for handling HRPT. The responsible official at the sending laboratory should verify that the intended carrier is able to provide this level of security.

The sending laboratory should initiate a chain-of-custody procedure that documents the control of the package containing HRPT materials during its transit and ensures the secure receipt of the material at the receiving facility. The sending laboratory should notify the receiving laboratory

promptly of the time that the shipment left the sending laboratory. The receiving laboratory should provide notification of successful receipt to the sending facility. Both laboratories should be prepared to independently follow up immediately if any shipment does not arrive as expected; at the same time, the incident should be reported to a higher authority.

6.6 Additional Good Practices for External Transfers

Transferring dangerous pathogens and toxins between facilities is a critical aspect of microbiological research and provides many more benefits than risks. But these materials are vulnerable to theft during the transfer process. Current international regulations, which primarily address transport safety, have only touched on pathogen transfer security.

Before implementing any transfer security mechanisms, it is important to consider the risk-to-benefit ratio. Transfer security mechanisms must work within a large body of safety regulations; allow for the efficient transfer of all materials, especially frozen materials; and remain cost-effective to not unduly hinder research and diagnostic work that are essential for public health.

It is prudent to limit the shipment of dangerous pathogens and toxins to small quantities. Under safety regulations, the maximum amount of dangerous animal or human pathogens or toxins that may be transferred is as follows:

- Passenger/cargo air—50 milliliters liquid/50 milligrams solid
- Cargo only—4 liters liquid/4 kilograms solid.

The opportunity for theft is greatly reduced by limiting the amount of time materials are in the custody of the commercial transfer system. Rapid shipments via air are recommended. Not only does this reduce exposure time, but air services may also have well controlled staging and bulk break areas that are restricted from the public.

Packaging requirements are usually dictated by transportation regulations and the carriers themselves. However, it is important that procedures be strictly followed in order to minimize the chance of breached containment. Also, the outside packaging should only provide the minimum identifying information required by the commercial carrier. The packaging should not attract any special attention.

Some air freight service providers provide a *constant surveillance* service. This service extends the time until delivery and increases the freight rate. Because of the additional transfer time, constant surveillance should *not* be used.

Although commercial carriers provide tracking services, it should be recognized that these services are not real-time nor do they guarantee custody over a package at all times. However, tracking does provide a relative knowledge of package location in the transfer system and can facilitate creating a documentation trail for facilities. Facilities should establish which individuals are responsible for package tracking and monitoring during the external material transfer process.

6.7 Reporting and Review

An accountable scientist should be responsible for reporting MCA status to his or her supervisor, to the head of the facility, or to the facility biosecurity officer. Annual reporting helps maintain current and accurate MCA information. The individual who receives the information from the accountable scientist should review the information for discrepancies and should be responsible for completing a summary report for submission to the appropriate officials. These summarizing reports should maintain the integrity of the information and enable rapid follow-up from the top down if additional detail becomes necessary.

Special reporting may be necessary under unusual conditions, such as a determination that material may be missing.

Laboratory notebooks, inventories, and databases that include material accountability information are subject to review at any time by personnel who are responsible for auditing.

Review of inventory records should be conducted at least annually and may be conducted randomly or without prior announcement. Methods used during physical review or during inventory reconciliation should include counts of the entire inventory or, for lower risk materials, a statistical sampling of records and repository materials. The head of the facility is responsible for ensuring that the reviews are accomplished. Inventories should be reconciled with material transfer records.

6.8 Transfer/Transport

Packaging and safety regulations governing material transfers are well established and accepted around the world. Shipping standards provide extensive guidance, documentation, and training for shippers, carriers, and receiving facilities. Similar to laboratory safety, transportation safety should be recognized as a priority in protecting the outside environment and people from the potential health risks posed by the movement of hazardous materials or dangerous goods such as dangerous pathogens and toxins.

Material transfers of dangerous pathogens and toxins should be in accordance with national regulations regarding marking, labeling, packaging, authorization, registration, biosecurity requirements, and export controls, if applicable.

Material transfers of dangerous pathogens and toxins should also be in accordance with any additional requirements imposed by the chosen commercial carrier.

6.9 Information Security

Any information created or stored as part of MCA that could directly or indirectly lead to the compromise of pathogens or toxins, especially HRPT materials, should be maintained securely. Such information is confidential and needs to be protected from unauthorized disclosure to anyone without a specific need to know.

Not only is the confidentiality of the information of concern but also its integrity. MCA information must be protected from unauthorized alteration or unintended deletion or corruption. Good information security practices include maintaining backups, authenticating input data, limiting access appropriately, and auditing records.

Information associated with MCA of MRPT or HRPT should be protected in a Limited Area. It may be protected in an Exclusion Area if this provides a measure of convenience to the staff; but if the Exclusion Area is a laboratory space, containment issues may be a problem.

Information considered sensitive and subject to information security measures includes laboratory notebooks with MCA records; material inventories, whether electronic or paper; and similar records. However, these records may also contain information that is not relevant to MCA. Divulging the unrelated information should only be done in a way that assures that sensitive information is protected.

It is important not to confuse the sensitivity of MCA information with other information concerns. For example, the technical results of experiments using the materials are an entirely different concern, and policies and procedures governing the handling of this type of information are beyond the scope of these guidelines.

7. Programme Management

7.1 Management Responsibilities

Laboratory biosecurity management guides and oversees the implementation of the laboratory biosecurity programme. It is the responsibility of the management to ensure that each component of the laboratory biosecurity system functions optimally and in a coordinated and consistent manner. To achieve this end, the management should identify and prioritize programme needs and allocate appropriate resources to meet those needs.

First, management should create a biosecurity plan that outlines the security measures that are implemented at the facility. The biosecurity plan should offer comprehensive guidance on the implementation of laboratory biosecurity at the facility and should address the policies and procedures associated with personnel management; physical security; and material control, accountability, and transfer. Management should clearly delineate the roles and responsibilities of laboratory personnel. To ensure that personnel are familiar with laboratory biosecurity, a variety of training programmes should also be implemented.

Management should also ensure continual improvement of the laboratory biosecurity system. Management should conduct routine self-assessments of the laboratory biosecurity system; subsequent management reviews should evaluate the findings of these assessments and propose actions to redress significant weaknesses. Actions should be both corrective and preventive in nature—that is, they should correct existing problems and anticipate and correct for new problems that may arise.

The following sections provide specific guidance on the management of the biosecurity programme.

7.2 Programme Planning

Every facility that stores, uses, or transports dangerous pathogens and toxins should develop and implement a laboratory biosecurity plan that establishes policies and procedures to ensure the security of areas that contain dangerous pathogens and toxins.

Laboratory biosecurity plans should describe in detail all the objectives, strategies, elements, and procedures associated with the facility's laboratory biosecurity system. The laboratory biosecurity plan should document the risk assessment process for the facility and describe the following elements of the laboratory biosecurity programme: management responsibilities, physical security, personnel management, and MCA.

All personnel should be trained to follow the laboratory biosecurity plan. Failure of an individual to follow the laboratory biosecurity requirements outlined in the laboratory biosecurity plan should result in disciplinary action.

The laboratory biosecurity plan should be annually reviewed, performance tested, and revised if necessary. This process should be repeated if a security incident occurs.

The laboratory biosecurity plan should:

- Describe how the facility meets specific security objectives
- Be based on a facility-specific risk assessment
- Tailor the guidance provided in the *Laboratory Biosecurity Implementation Guidelines*, including laboratory biosecurity programme management, physical security, personnel security, information security, MCA, and material transfer security, to operations at a specific facility
- Describe, justify, and document the graded protection provided to dangerous pathogens and toxins and indicate how the system will detect, deter, and respond to unauthorized access to these agents
- Contain notification guidance for providing oral and written reports in the event of the theft, loss, or release of dangerous pathogens and toxins
- Contain an explanation of the laboratory biosecurity training to be received by all personnel
- Contain provisions for routine cleaning, maintenance, and repairs of restricted areas
- Contain procedures for laboratory biosecurity programme audits
- Contain an incident response planning section that should:
 - Be coordinated with the facility's emergency response plans and its biosafety plan
 - Include responses to the following types of incidents: biocontainment breaches, laboratory biosecurity breaches, inventory violations, material transfer violations, computer security breaches, and nonbiological security incidents (e.g., violence in the workplace, severe weather, power outages, natural disasters) if not already addressed by the facility's emergency response plan
 - Instruct facility personnel, including its guard forces, local law enforcement, and emergency responders, on the exact procedures to follow in the event of an incident
 - Indicate, when appropriate, what memoranda of understanding are in place with local law enforcement and emergency response agencies and officials
 - Develop a public relations strategy to communicate the facts associated with an incident and its consequences to the public
 - Develop a chain of command for incident reporting at the facility level

- Include actions required to protect forensic evidence of a theft or an attempted theft

7.3 Roles and Responsibilities

The laboratory biosecurity programme should outline individual biosecurity responsibilities. These roles and responsibilities include management responsibilities; physical security; personnel management; and material control, accountability, and transfer.

7.3.1 Laboratory Director

- Management responsibilities
 - Ensures that effective laboratory biosecurity is implemented at the facility.
 - Is responsible for incident control and serves as incident response chief; may delegate on-scene incident response control to other administrative staff

7.3.2 Laboratory Biosecurity Officer

- Management responsibilities
 - Works with local line managers and the laboratory biosafety officer to ensure the laboratory is adhering to policies on biosafety and biosecurity
 - Manages and directs the implementation of physical security and personnel security at the facility
 - Coordinates with the laboratory biosafety officer and the emergency operations centre or emergency responders regarding security incidents
 - Works closely with diagnostic, biological research staff to ensure that laboratory biosecurity levels are adequate for campus laboratories and buildings
 - Establishes, develops, maintains, and updates criteria for identifying and analyzing trends in laboratory biosecurity violations and other lapses in laboratory biosecurity in achieving laboratory biosecurity objectives and goals
 - Conducts self-assessments
 - Maintains the laboratory biosecurity plan

7.3.3 Personnel Management

- Coordinates required background investigations and adjudication

- Implements badging and visitor control requirements
- Laboratory Biosafety Officer
- Management responsibilities within the context of biosecurity
- Works with local line managers and the laboratory biosecurity officer to ensure laboratories are adhering to policies on biosafety and biosecurity
- Coordinates with the emergency operations centre or emergency responders as appropriate regarding safety incidents
- Works closely with diagnostic, biological research staff to ensure laboratory biosafety levels are adequate for campus laboratories
- Ensures that laboratory staff maintain appropriate vaccination schedules and reports lapses to personnel management to ensure action is taken as necessary to preclude access
- Maintains the laboratory biosafety plan

7.3.4 Information Security System Administrator

- Management responsibilities
 - Serves as the main point of contact for information security issues; implements information security policies and participates in the development of laboratory biosecurity plans
 - Monitors local computer security activities, responds to computer security incidents with the appropriate headquarters oversight office, and ensures that there is a local understanding of computer security policies and procedures

7.3.5 Line Managers

- Management responsibilities
 - Implement operational laboratory biosecurity programmes with direct oversight assigned to researchers and diagnosticians
 - Provide resources for training, implementation, and monitoring of laboratory biosecurity policies and programmes; ensure that personnel receive annual comprehensive laboratory biosecurity training
 - Conduct in-processing (orientation) and out-processing (termination) briefings as required

- Perform review and approval of information for public release
- Monitor psychological and physical health and well being of those authorized to access dangerous pathogens and toxins
- Manage the security infraction process
- Instill and maintain continued awareness of laboratory biosecurity requirements and the importance of laboratory biosecurity

7.3.6 Individual Researchers and Diagnosticians

- Management responsibilities
 - Have the primary role for day-to-day biosafety and biosecurity practices related to inventory management
- Material Control and Accountability
 - Oversee the use of dangerous pathogens and toxins by technicians and other support staff
 - Ensure material transfers follow procedures

7.3.7 Response Force Team

- Respond to potential laboratory biosecurity incidents
- Perform routine security functions, such as:
 - restrict access at entry gates or entrances to restricted areas to authorized vehicles and personnel
 - monitor parking areas and the overall campus as a means of deterring illicit acts as well as to ensure no unauthorized vehicles or personnel are present
 - provide escort in unrestricted areas, such as into the parking lot after hours
 - provide escort in restricted areas, provided all personnel management requirements are satisfied
- Monitor and assess alarms produced by any electronic intrusion detection system

7.3.8 All Personnel

- Responsible for understanding and complying with all laboratory biosecurity policies and procedures

7.4 Laboratory Biosecurity Training

Each facility should provide laboratory biosecurity training to each individual on personal responsibilities associated with working in or visiting areas where dangerous pathogens and toxins or restricted information are stored or handled. This training should be provided at the time of an individual's initial assignment to an area where dangerous pathogens and toxins are present or when access to restricted information is required. Records should be maintained that identify the individual, the date of training, and the means used to verify that the individual understood the training.

Laboratory biosecurity training is an integral part of a laboratory biosecurity programme. All personnel should be required to complete annual laboratory biosecurity training. In addition, all management should be required to complete annual supervisory reporting requirements training. Appropriate personnel should complete the annual response force training.

7.4.1 Annual Comprehensive Training

Annual comprehensive laboratory biosecurity training should be required for each employee before he or she reports for routine duties. Employees should not have access to computer systems with sensitive information or unescorted access to Limited and Exclusion Areas until this training is completed. Failure to attend this training annually should result in loss of access to Limited and Exclusion Areas until the training has been completed. Training records should be maintained. The annual comprehensive laboratory biosecurity training should address the laboratory biosecurity-related topics described below.

7.4.1.1 Statutory Laboratory Biosecurity Requirements

All employees should be informed of any statutory laboratory biosecurity requirements that may exist at the local, regional, or national levels and of their responsibilities for meeting those requirements.

7.4.1.2 Physical Security Measures

All employees should be informed of the defined restricted access areas at facilities—Property Protection, Limited, and Exclusion Areas—and the applicable access control procedures for each area.

Every employee should be informed of all other physical security policies and procedures at the facility regarding access hours, visitor logs, vehicle security, tailgating prohibition, reporting suspicious activities and unauthorized individuals, prohibited articles, animal and supply handling, and the need to consolidate dangerous pathogens and toxins to the extent possible.

7.4.1.3 Personnel Management Measures

All employees should be informed of the following personnel security measures at facilities: position designations, background checks and/or personality tests, derogatory information affecting access, badges, visitors, host responsibilities, escorting, and foreign travel.

7.4.1.4 Information Security Measures

All employees should be informed of the following information security measures at facilities: types of restricted information, restricted information access and protection requirements, network protections, user desktop system protections, remote access, and wireless networking.

7.4.1.5 Laboratory Biosecurity Incident Reporting

All employees should be informed of the types of laboratory biosecurity incidents and the associated reporting procedures.

7.4.1.6 Laboratory Biosecurity Violations

All employees should be informed of the types of laboratory biosecurity violations and the associated disciplinary actions.

7.4.1.7 Media and Public Requests

All employees should be informed of the appropriate laboratory biosecurity procedures with regard to being contacted by the media or the public.

7.4.2 Annual Supervisory Training

Supervisory training should be required annually for the managers at facilities. The training should inform managers of their reporting responsibilities associated with derogatory information and should encourage them to report any information that raises doubts about an employee's continued eligibility for access to dangerous pathogens and toxins and restricted information.

Supervisors should also be trained to monitor the physical and mental health of those working with dangerous pathogens and toxins. If an employee appears to be in poor health, it is possible that the employee may pose a safety or even a security threat and should be counseled or required to not work with dangerous pathogens or toxins until he or she has recovered.

Supervisors should provide access to any form of employee assistance programme materials (See Chapter 5.) and be trained to spot abnormal behaviours that may indicate a need for these types of services.

Supervisors should be trained to manage the facility's property that is typically issued to employees, especially those items that are directly related to access control or other security functions.

Supervisors should be trained to manage personnel background checks, to maintain training and immunization records, and to perform review and approval for information for public release. Some of these functions may reside in another area, such as in a personnel management organisation. If so, supervisors should be aware of the compliance of their employees in meeting these requirements.

7.4.3 Annual Response Force Training

If a facility has a response force, an overall objective of the annual response force training and qualification programme should be to develop and maintain, in an effective and efficient manner, the competencies needed by the on-site response force to perform the tasks required to fulfill the on-site response force mission.

7.4.3.1 Training Course

Prior to initial assignment to duty, an on-site response force officer should successfully complete the basic response force training. Facility-specific training requirements should include the location of, and security and safety issues associated with, any dangerous pathogens and toxins at the facility as well as who are the accountable scientists. The response force training should also include, but not be limited to, the following types of instruction: orientation and standards of conduct; laboratory biosecurity education and operations; dangerous pathogens and toxins protection requirements and issues surrounding access to restricted areas during an emergency; restricted information protection requirements; response to and reporting of incidents of laboratory biosecurity concern; protection of government property; physical fitness training; facility operations familiarity; safety training; legal requirements and responsibilities; weaponless self-defence; use-of-force policy; communications, including methods and procedures; vehicle operations, including methods and procedures; post and patrol operations; and use of assigned personal protective equipment.

7.4.3.2 Training Exercises

Exercises of various types should be included in the training process for the purpose of achieving and maintaining skills and for assessing individual and team competency levels. The types and frequency of training exercises should be approved by the facility laboratory biosecurity officer. At a minimum, the following elements should be included in the training exercise programme:

- Exercises involving each response force officer's shift should be conducted monthly. These exercises should be planned and conducted so as to provide facility-specific training.
- The facility laboratory biosecurity officer should request any local law enforcement or military base personnel who would assist the on-site response force during a facility laboratory biosecurity incident to participate in training exercises at least annually.
- Reports of each training exercise, summarizing results and problem areas, should be prepared for management review to aid in planning response force activities and developing corrective actions.

7.5 Self-Assessments

Self-assessments are internal audits that provide facilities with internal monitoring of laboratory biosecurity programmes to ensure ongoing compliance with laboratory biosecurity requirements. A self-assessment should cover the following laboratory biosecurity elements: management

responsibilities; physical security; personnel management; and material control, accountability, and transfer operations.

Depending on a country's laws and regulations, facilities may also be required to submit to audits by an external agency. Self-assessment and external audit requirements should be documented in the biosecurity plan.

7.5.1 Programme Management

The programme management self-assessment should ensure that biosecurity, emergency, and incident response plans are regularly reviewed and should ensure compliance with training requirements. In addition, this self-assessment should ensure that restricted information is secured appropriately and that records are accurate and up to date.

7.5.2 Physical Security

The physical security self-assessment should ensure that all security devices are operational and that maintenance is performed regularly on an as-needed basis. This should also include an assessment of response forces to ensure training is conducted regularly and that the force is prepared to respond.

7.5.3 Personnel Management

The personnel management self-assessment should ensure that granting of personnel access to facilities is appropriate and up to date. Personnel access applies to all employees and visitors. The self-assessment should address the components of the facility's personnel management programme, which may include the following key elements: access authorization, visitors, badges, hosting, escorting, and travel. The self-assessment should also include a review of all access logs, both electronic and handwritten.

7.5.4 Material Control and Accountability

The MCA self-assessment should ensure that material control, accountability, and transfer security techniques that are applied to dangerous pathogens and toxins are effective. The self-assessment should also address the following key elements of material transfer: chain of custody, shipping and receiving, and material accountability records.

7.5.5 Corrective Action Plans

Corrective actions should be undertaken and documented whenever a self-assessment report contains one or more findings of error or ineffectiveness. The corrective action plans should include actions to be taken, organisations and individuals responsible for each action, the schedule (including key milestones), actions to address root causes, a process for tracking

actions to closure, and steps to verify effectiveness of actions prior to closure. It is essential that upper management be involved in corrective actions to resolve findings and thereby improve the effectiveness and efficiency of the laboratory biosecurity programme. It is necessary to have a standard timeline through which these findings are resolved. Once the corrective action has been taken and tests for effectiveness have been conducted, a record of closure should be created.

Appendix A. Information Security

A.1 Handling of Sensitive Information

Sensitive information requires certain security precautions be taken in order to avoid inadvertent release to unauthorized individuals. Sensitive information needs be restricted in a manner that keeps it from those who do not have a need to know, i.e., a legitimate business-related reason for having access to the information.

A.1.1 Review and Approval of Information Prior to Public Release

A process should be established for review and approval of all information, including hard copies and digital publications, prior to public release. The process should include a list of personnel authorized to review and approve information for release and clear policies and procedures for posting Web site content.

A.1.2 Access to Restricted Information

Restricted information should only be available to those individuals who have a need to know. If an individual has a legitimate business-related reason for having access to the information, he or she has a need to know. The responsibility for determining whether an individual needs access to specific information should reside with the individual who currently has authorized possession, knowledge, or control of the information—and not with the prospective recipient.

A.1.3 Marking Sensitive Information as Restricted

Information that has been determined to be sensitive information should be clearly marked as *Restricted*. Marking in this manner is intended to alert those who do not have a need to know that reading or possessing such material would be unauthorized and subject to disciplinary action.

Documents

Documents should have a cover page that is marked *Restricted*, and the back cover should be blank.

Internal pages of the document should be marked *Restricted* at the top and bottom of each page in letters clearly distinguishable from the text.

Removable Electronic Media

Removable electronic media containing sensitive information should be labeled *Restricted*. The label should be clearly visible and should be applied in a way that it does not interfere with the drive mechanism. Removable electronic media includes CDs, DVDs, pen drives, floppy disks,

digital tape cassettes, removable hard drives, and any other device on which data can be stored and that normally is removable from the system by the user or operator.

Blueprints, Engineering Drawings, Charts, and Maps

Blueprints, engineering drawings, charts, and maps containing sensitive information should be marked *Restricted* at the top and bottom of each page. If the blueprints, drawings, charts, or maps are large enough that they are likely to be rolled or folded, *Restricted* should be placed so that it will be visible when the item is rolled or folded.

Photographs and Negatives

Photographs containing sensitive information should be marked *Restricted* on the face, if possible. If this cannot be done, the marking should be placed on the reverse side. Negatives containing sensitive information should have *Restricted* marked on their storage container, e.g., an envelope.

A.1.4 Storage Rules for Restricted Information

Sensitive information, both in hard copy and electronic form, should be physically protected and should be stored in a Limited Area. An Exclusion Area is also an acceptable storage location, but a high containment laboratory should only be used as a storage area for sensitive information when absolutely necessary due to containment issues. Storing sensitive information in an unrestricted area should only occur when additional protections are taken, e.g., storing in a locked container when not under the personal control of an individual with a need to know.

Information handled electronically and transmitted over the network is at a higher risk of being released or altered and should therefore only be transmitted electronically when encrypted. If sensitive information resides on an institution's network, access to the information should be restricted with passwords, and the network should be protected with a high level of electronic protection, such as firewalls, intrusion detection, defence-in-depth, isolation of sensitive information, and good practices network administration, to ensure the integrity of sensitive information and to prevent unauthorized access into these systems. Protection methods should be reviewed and system auditing performed regularly in order to properly maintain protection of these systems.

The physical elements of the network systems that store and transmit sensitive information or that have direct access to sensitive information should be secured within a Limited Area or an Exclusion Area. Network or security system control rooms should reside in areas that restrict access to those with a need to know.

A.1.5 Communicating Sensitive Information

Sensitive information may be communicated in the following ways:

- From person to person in direct contact with one another

- Over a landline telephone
- Via a reliable mail service, including overnight mail service by FedEx or another international carrier, with no external markings that would indicate the material is sensitive
- Via fax machine when an authorized recipient is waiting at the receiving machine from the beginning of the transmission process until it is complete
- Within the institution's internal email domain ([...]*@*[institution name].[extension]) provided that the internal domain is protected from external intrusion and that the email is not routed to anyone outside this domain
- Across unprotected networks, e.g., the institution's network if it is not sufficiently secure or between the institution's network and an outside email recipient, provided that the sensitive data is encrypted and authenticated

A.1.5.1 Telephone or Videoconference

Although sensitive information may be discussed on landline telephones, sensitive information should not be discussed on cellular phones.

Sensitive information should not be transmitted via open network communication channels, including online videoconferencing, unless such a conference is held on a restricted network.

A.1.5.2 Mail

Transmission of sensitive information should be done in a manner that informs those with a need to know of the level of sensitivity while not advertising the fact to the general public. It is also important to use a reliable means of shipping. These considerations help to avoid unauthorized disclosure or dissemination of sensitive information.

Internal Mail

Before transmitting sensitive information through an internal mail system, the information should have appropriate markings and a cover sheet and be placed in an envelope marked *Restricted*.

External Mail

Sensitive information sent outside the institution's premises should be transmitted via a reliable mail service, including overnight mail service by FedEx or another international carrier. The outer wrapping should not be marked in a manner that would reveal the contents of the envelope or package to unauthorized personnel.

A.1.5.3 Faxing

Prior to faxing sensitive information, the sender should confirm that an authorized person will be present at the receiving end for the duration of the transmission, or the sender should verify that the receiving facility is protected in a manner sufficient to preclude unauthorized access to the transmitted material.

A.1.5.4 Electronic Transmission

Sensitive information should be encrypted and authenticated if it is sent outside the institution's protected network or within an institution's network if it is insufficiently protected. Sensitive information should never be communicated over wireless technologies such as cellular or cordless telephones or other wireless data transmission devices or devices using a cellular, radiofrequency, or satellite modem or using infrared connectivity.

A.1.5.5 Reproduction

Documents may be reproduced for business purposes without the permission of the originator. Copies should be protected in the same manner as the original. In the event of a copy machine malfunction, the copy machine should be cleared and all paper paths checked for papers containing sensitive information.

A.1.6 Destruction of Sensitive Information

Sensitive information should be destroyed by shredding or another method of comprehensive destruction, such as burning. Paper containing sensitive information should not be recycled and should not be commingled with nonsensitive information. Its destruction should be carried out by authorized personnel and its security maintained until it has been destroyed.

Merely deleting, erasing, or formatting will not sufficiently remove sensitive information from electronic storage formats. Instead, files should be removed by using multiple passes, a minimum of ten times, of a hard drive-wiping programme.

Electronic or removable media should be physically damaged to the point of inoperability via shredding, degaussing, melting, or other such methods before disposal.

Appendix B. Network Security

B.1 Network Management

B.1.1 Router Configurations

External network routers can offer unintended access into a network by not being properly configured. Numerous opportunities for router exploitation exist that could enable access from an external network like the Internet into the internal network. Using such configuration errors an unauthorized person could potentially access internal network information, which may be sensitive in nature. There have been numerous documented cases of router exploitation being used to gain illicit access into networks.

Network routers should be the first layer of protection on any network. Most routers can be configured to provide higher security by performing simple administrative tasks. Disabling the ability to provide remote administration and other unnecessary administrative tools, such as the simple network management protocol (SNMP), and using a nondefault and good quality passwords is advisable. Additionally, a router can be used as a network protection device by utilizing access control lists and limiting access to and from the network.

B.1.2 Public Information

Web sites and other public sources of information can allow an unauthorized person to gain insider knowledge. This knowledge can be used for social engineering; that is to provide false credentials to gain access to the internal network or to other protected information by exploiting human nature. Also, public information sources can be used to enhance the network surveillance techniques used by adversaries to collect information that can be used for an attack on an institution's network.

All information should be reviewed for public release before being presented on a public webpage or any other public network data sharing system, like a public file transfer site using file transfer protocol (FTP). See Appendix C for additional details on protecting sensitive information.

B.1.3 Firewalls

A firewall is a bastion of safety for the internal network by protecting it from the external network or Internet. However, an improperly configured firewall or a firewall placed incorrectly within the network topology can provide a false sense of security. Firewalls, like routers have been repeatedly exploited by unauthorized persons who are then able to gain illicit access to the internal network and subsequently all information that resides within the internal network.

A firewall should be used as the main layer of defence behind the router. Like the router, it should only provide limited administrator access and be configured to the highest security level possible. The firewall itself should be designed to strictly limit or deny all traffic from the external network incoming to the internal network. The traffic from the internal network to the external network should ideally be limited to only the services required for authorized user use.

B.1.4 Dial-In Access

Dial-in systems or modem banks can offer a conduit into the internal network for both legitimate work and illicit use by unauthorized users. Historically, modems have offered easy targets for an outsider to gain inside access. A war dialer is a computer programme used to identify the phone numbers that can successfully make a connection with a computer modem; they have been used since the introduction of modems (early 1970s) to allow malicious access into networks. War dialers are still widely used today for malicious access and modern modems do not offer any more security than those of the past. Remote access systems, which handle call routing of the modem system, can offer the needed level of protection, but are often not installed using all of the methods required to make them fully secure. In general, the use of dial-in modems to access information on the institution's internal network is highly discouraged. The use of a virtual private network (VPN) system is preferable. (See Section B.1.5 below for discussion on VPN.) However, if dial-in capability is required, a variety of protection mechanisms should be applied. The dial-in modem systems must be accompanied by a secure remote access management system, which would ideally be located on an isolated network segment with specific firewalls and access controls configured to limit access to the internal network to those with authorization. If required, the users' system should be isolated from the network. Users who require dial-out access to connect to other networks should have the modem's dial-in ability disabled. Also these systems should ideally have a personal firewall.

B.1.5 Virtual Private Network (VPN)

B.1.5.1 Remote Access

A VPN offers an alternative to dial-in modems for remote users who need to gain access to the internal network. Like most networking systems, VPNs can be configured incorrectly in a manner that would enable an unauthorized user to gain illicit access onto the internal network. To prevent unauthorized access, remote access VPNs should be configured in conjunction with a firewall and in such a way as to ensure remote users follow all authentication protocols.

The remote user's computer must also be protected from external exploitation, as any access to the remote user's computer would potentially allow access into the internal network. Personal firewalls, virus protection and user understanding are critical to a secure remote-access VPN installation.

B.1.5.2 Remote Sites

A VPN can also be used to join two or more geographically separate networks using a public infrastructure like the Internet. For those organisations that require connectivity between two remote networks, VPNs, working over the Internet, are generally less expensive than a direct connection (dedicated phone line, cable, or fiber) between two remote networks. However, when incorrectly configured, VPNs can be a security risk to both networks. Each network must provide the same level of security to avoid creating a backdoor into the network. Both VPN systems also need to be configured to the highest level of security, like the router and firewall. That is, remote administration should be disabled or limited and passwords should be reset from the default and be of good quality. The VPN security association mechanisms should also be verified to confirm that neither end point could be forced into an unencrypted mode.

B.1.6 Servers

All servers should be configured to the highest level of security possible. This is true for both internal servers and external servers. Server processes can often be used as conduits for unauthorized system access and can enable such an unauthorized presence to obtain additional access to other devices on the network. The core operating system should be secured, and any running service should be a verified secure version.

B.1.6.1 Web

Web servers and Web applications are currently among the most widely attacked and compromised services. These services, especially when installed on an external network, can be trivial to bypass. It is critical to use only well verified Web servers and to test any and all applications for problems. Web applications should be screened for buffer overflows, injection, and other common problems.

B.1.6.2 Email

The email server has historically been a heavily attacked service. Modern email servers are far better than the early versions; but like the Web server, it is critical to verify the server is not prone to compromise.

Email itself is also a potential problem for the overall security of the network. It is advisable that all incoming email be streamed through a central server and checked for potential viruses and Trojan programmes. Also, any email of a sensitive nature should not be stored or transmitted on an external server without encryption.

B.1.6.3 Database

Databases are a new favourite attack point for those who wish to gain unauthorized network access. This access can be obtained via Web-based database applications or by a network

connection to any database. As sensitive information is often stored within a database, preventing database (or SQL database query language) injection to gain illicit access is very important, and testing to ensure databases are secure should be done routinely.

The operating system in which the database is running can be a potential concern and should be configured like any other server; that is to the highest level of security possible. A database containing sensitive information, like a pathogen inventory or user access rights, should not be on the general internal network. Such databases should be on separate access-controlled networks to which only users with a specific need to know have access.

B.1.7 Wireless Local Area Networks

A wireless local area network (LAN) can create additional security issues for a network. The use of a wireless system reduces the need for physical access to the network infrastructure, thereby making it much more available to a wider group of individuals, both authorized and unauthorized. Wireless Ethernet, Wi-Fi (wireless fidelity), or IEEE (Institute of Electrical and Electronics Engineers) Standard 802.11, devices can be highly useful; but before such a network is installed, it is necessary to understand the potential risk. With a wireless network, the risks include: unauthorized network access, unauthorized review of transmitted data, and the injection of false data. Wireless networks can also be disrupted by the use of external radio signals.

Using additional security mechanisms like installing Wi-Fi Protection Access (WPA) with 802.1x or a VPN/firewall and creating an isolated wireless network segment can mitigate the risks of deploying a wireless network. However, depending on the nature of the data and the network, wireless should not be used in some areas. For example, a physical security system should not be running along a wireless network.

B.2 Users

All users working on a facility's network should have a basic understanding of network security and the potential risks associated with not following the network and desktop policies designed to protect the network.

B.2.1 Network Access Layers

B.2.1.1 Domains

The facility's network should ideally limit the users' access to only the information that is directly related to their work, i.e., the information the user has a need to know. The use of network domain controllers can aid in achieving this objective. However, if a domain controller is not properly configured, an insider with limited access may be able to increase his or her level of access. Care in the installation and maintenance of a network domain is essential to avoid security vulnerabilities.

B.2.1.2 Virtual Local Area Networks

A virtual local area network (vLAN) can be used to create a more strict isolation of networks. A vLAN can be used to reduce the overall overhead associated with multiple networks but nonetheless creates a boundary between each network LAN. A well-configured vLAN is not prone to security issues, but the installation and the level of ability required for users to work on multiple vLANs may be more demanding than more conventional systems. Both of these issues must be addressed prior to designing a vLAN into the network.

B.2.2 Desktop Security

B.2.2.1 Passwords

All systems should have passwords. Password protection is particularly critical to any system that stores or otherwise provides access to sensitive information. Usernames and passwords should be used to authenticate users before granting access to any sensitive information. Passwords should never be dictionary words or common names, nor should they be the same as the login name. Ideally, passwords would be eight characters or more. If the system is in an open or public area, the system should also be protected by a boot-up password. Passwords should not be kept anywhere near the system or anywhere in the open. Systems that are intended for the use of the general public, such as at an informational kiosk, should be isolated from the internal network and should not have any access to sensitive information.

B.2.2.2 Desktop Management

Network administrators will often utilize a desktop management system to enable automatic patching and upgrading of the facility's network. Because continuous upgrading and patching of systems is critical to maintaining the overall security of the network, such an automated system is considered a good administrative practice. It should be verified, however, that such a system does not disrupt the users' day-to-day work nor provide an additional risk to the network. The network administrators should have a good understanding of desktop management systems before deploying one across the entire facility network.

B.2.2.3 Virus Protection

All systems should be reviewed, as appropriate, for malicious code and viruses. This includes incoming email messages and any downloaded information or software. Antivirus software should be updated and run automatically. Any workstation that is used on multiple networks should contain a personal firewall and all systems should have some form of virus protection.

B.2.3 Wireless Personal Area Network

As with a wireless LAN, the use of a wireless personal area network (PAN) device should be considered a potential risk to network security. The use of devices incorporating such wireless technologies as Bluetooth should be limited to only those systems that do not store or otherwise provide access to sensitive information. Also, as the biggest risk of using Bluetooth devices is the initial pairing of such devices, the devices should only be paired within a physically secure, restricted area; and the range of such devices should be limited.

Cellular phone systems can also be used to compromise the security of information. The use of cellular and other wireless telephony devices should be prohibited for discussions of a sensitive nature and for the transmission of sensitive information.

Appendix C. Biosecurity by Baseline Risk Category

C.1 Introduction

Risk mitigation measures (physical; personnel; and material control, accountability, and transport) should become more robust with greater baseline risk for the pathogens and toxins held at a facility. This appendix describes only those biosecurity measures that are implemented in a graded manner, emphasizing the differences between the various risk levels. Each level presumes that those policies and procedures that apply across risk levels as described in the main text have been implemented and that those features of the next lower risk level are also in place. In other words, the risk mitigation measures build upon each other and upon the general policies and procedures described in the main text.

C.2 LRPT

See Chapter 3 for a complete description of baseline pathogen and toxin risk categories.

C.2.1 Physical Security

See Chapter 4 for a complete description of physical security recommendations.

C.2.1.1 Property Protection Areas

The Property Protection Area is defined by the outermost perimeter of a facility's campus or by the facility walls if there is no discernible exterior perimeter belonging to the facility. A Property Protection Area is intended to protect against damage, destruction, and theft of facility property. A perimeter fence may establish the Property Protection Area. Such a fence defines the boundaries of the campus as well as providing a means to control personnel and vehicle access. For facilities that hold assets of only low or moderate risk, signage may provide sufficient property demarcation. A Property Protection Area can contain both Limited Areas and buildings that require little or no protection measures, such as warehouses and public access areas. LRPT may be used and stored in a Property Protection Area and should be protected to the degree provided by good biosafety practice.

C.2.2 Personnel Management

See Chapter 5 for a complete description of personnel management recommendations.

Personnel authorized to work with or handle LRPT should be considered to hold Low Risk positions.

C.2.3 Material Control and Accountability

See Chapter 6 for a complete description of material control, accountability, and transport recommendations.

A laboratory notebook maintained by the accountable scientist should document the stocks and use of materials under his purview. Laboratory management should keep a record of where LRPT materials are stored and used and a record of the corresponding accountable scientists.

The transport of LRPT should also be documented in the laboratory notebook. Recorded information should specify what was shipped and should include the date and destination of the shipment, the name of the person expected to receive the shipment, the name of the carrier used to ship the material, and the tracking information for the shipment.

C.3 MRPT

C.3.1 Physical Security

C.3.1.1 Limited Areas

A Limited Area is appropriate for storage and use of MRPT. A Limited Area resides within a Property Protection Area. An entire building may be designated as a Limited Area, or individual rooms or laboratories that reside within a building may be designated as separate Limited Areas.

A Limited Area has access controls and intrusion detection in place to provide reasonable assurance that only authorized personnel enter and exit the area. Those who are not authorized for routine access to a Limited Area should be escorted by an authorized individual and should be required to sign a visitor log.

Access to a Limited Area requires access authorization and a unique item, such as a physical or electronic key, or accompaniment by an authorized escort. Physical keys should be controlled in such a way as to ensure that they are issued only to those individuals who have a legitimate need to have unlimited access to a Limited Area and that they are returned when this access is no longer needed, such as upon transfer or termination.

C.3.1.2 Intrusion Detection

Limited Areas should be monitored regularly, either electronically or by facility personnel, for signs of unauthorized access. If unauthorized access is suspected, it should be investigated (assessed). If the investigation cannot determine whether the breach was accidental or intentional or if the breach is clearly intentional, the proper authorities, including those qualified as response forces, should be summoned to investigate the situation further.

C.3.1.3 Structural Issues

A Limited Area should have balanced strength of construction, i.e., the door should be essentially as difficult to get through as the adjacent wall. At a minimum, all doors and windows should be closed and locked during nonbusiness hours, and the doors and locks should be robust.

Panic hardware or other emergency exit mechanisms used on emergency doors located in a Limited or Exclusion Area should be operable only from inside the building or room and should meet all applicable life-safety codes.

C.3.1.4 Policies and Procedures

Visitors to a Limited or Exclusion Area should fill out a visitor log or be logged into the area electronically.

Tailgating, defined as more than one person passing through a controlled access point using a single key, should be prohibited.

C.3.2 Personnel Management

C.3.2.1 Screening

Personnel authorized to work with or handle MRPT should be considered to hold Moderate Risk positions.

A pre-qualification cheque should be conducted prior to offering any individual a Moderate Risk position.

Once an individual has accepted a Moderate Risk position, an employment screening should be conducted in an effort to establish the individual's reliability and character. An evaluation of this screening should be completed and the individual should be formally authorized to enter the appropriate Limited Areas to work prior to receiving a key for those areas. Until formal authorization is granted, the individual should remain under escort within Limited Areas.

C.3.2.2 Visitors

Visitors who require unescorted access to any Limited Area should be held to the same standard as employees who regularly work in these areas.

Within a Limited Area, the visitor-to-escort ratio should not exceed 8-to-1. Within a Limited Area, administrative escorting procedures should be allowed; for example, an individual under escort may go to the lavatory or get something to drink on the same floor without the escort in attendance. The escort must know where the individual is, and the individual must understand that he or she is not permitted to conduct any other than the prearranged activities and should return to the escort promptly.

C.3.2.3 Badges

Institutions that hold MRPT or higher risk pathogens or toxins should ask their employees and visitors to wear identification badges. Visitor badges should be returned daily or upon conclusion of a visit that is shorter than a day.

C.3.2.4 Access Control Management

Controlled keys and identification badges should be returned to the institution upon an employee's termination or transfer. Any electronic system access should also be actively managed to provide only the level of network access that is necessary and sufficient for the employee to work efficiently.

C.3.3 Material Control and Accountability

MCA measures for MRPT materials are based on those for LRPT, such as maintaining information in laboratory notebooks, but include additional measures. Inventories should be maintained in secure, limited-access databases that are consistent throughout the facility.

Information about the transfer of MRPT should be included in the laboratory inventory database. Paper documentation of a transfer, such as carrier receipts, should be kept for historical documentation of the transfer. If temporary storage needs to be provided for packages awaiting transit, the security should be equivalent to that for the Limited Areas used for handling MRPT. The accountable scientist responsible for shipping the materials should have knowledge of the professional nature of the receiving laboratory and should know that the individual receiving the material is qualified to work with MRPT.

C.4 HRPT

C.4.1 Physical Security

C.4.1.1 Exclusion Areas

An Exclusion Area is appropriate for the storage and handling of HRPT and should also be used to contain animals infected with an HRPT. Access to an Exclusion Area requires a unique item and unique knowledge, such as a physical key and positive identification provided by a guard or an electronic key and a PIN. Individuals who have a legitimate purpose for access but who do not have routine access privileges may be accompanied by an authorized escort. Both routine and visiting personnel should be required to sign a log upon entry and exit if electronic logging is not provided by the access control system.

An Exclusion Area generally has a smaller set of individuals who are authorized to enter than does a Limited Area. The keys to an Exclusion Area should be controlled, and each individual

in possession of a key should be documented. Storage containers such as freezers or refrigerators that are located within a Limited Area and that are under the control of both a unique item and unique knowledge may also be considered Exclusion Areas.

C.4.1.2 Intrusion Detection

Restricted areas should be monitored for unauthorized access. For those facilities maintaining Exclusion Areas for the storage and use of HRPT, it is recommended that security personnel monitor all entrances and exits either in person or through the use of an electronic intrusion detection system.

Sensors beyond what might be employed in a Limited Area may be used to detect an unauthorized attempt at access. Such sensors might include: glass break sensors on windows and motion detection or volumetric sensors within the room.

If the facility holds HRPT and local law enforcement cannot respond to an alarm on-site within a reasonable period of time, the facility might consider employment of an on-site guard force.

C.4.1.3 Structural Issues

The perimeter that forms the envelope of an Exclusion Area should, to the extent possible, be comprised of equivalently strong elements. For instance, the door should be as difficult to penetrate as the wall. Windows and other penetrations should be limited but when provided should be protected with either wire mesh (preferably 9-gauge stainless steel mesh fastened securely to the inside of the area) or glass break sensors. All exterior glass windows, hatches, ducts, or vents that form part of the perimeter of an Exclusion Area should be fortified to meet or exceed the strength of the surrounding wall or door.

C.4.1.4 Policies and Procedures

Facilities with Exclusion Areas might consider implementing vehicle controls, including identification tags on vehicles or parking passes, and monitoring parking areas for authorization.

Video and other recording devices might be restricted to use by only those with prior authorization in order to prevent documentation of the facility's security system implementation.

C.4.2 Personnel Management

C.4.2.1 Screening

Personnel authorized to work with or handle HRPT should be considered to hold High Risk positions.

A pre-qualification cheque should be conducted prior to offering any individual a High Risk position.

A more thorough employment screening should be conducted once the individual has accepted a High Risk position and should be more comprehensive than that conducted for those holding Moderate Risk positions, e.g., by reviewing more years in the past, interviewing a broader range of associates, and/or looking into a wider variety of issues. An evaluation of this screening should be completed and the individual should be formally authorized to enter the appropriate Limited or Exclusion Areas to work prior to receiving a key for those areas. Until formal authorization has been granted, the individual should remain under escort within Limited and Exclusion Areas.

C.4.2.2 Visitors

A working visitor who requires unescorted access to a Limited or Exclusion Area should be held to the same standards as employees who regularly work in the area. Casual visitors to an Exclusion Area are discouraged.

Within an Exclusion Area, the visitor-to-escort ratio should not exceed 1-to-1 for working visitors and 4-to-1 for tours or other demonstration-related activities. The escort should remain with the visitors at all times while inside an Exclusion Area, maintaining verbal and visual contact at all times.

C.4.3 Material Control and Accountability

All MCA measures for HRPT are based on those for MRPT, with the following additional guidelines:

Transfer should be authorized and approved by the facility's biosafety officer or another designated responsible official before the material ships. The designated responsible official for the sending laboratory should confirm that both the receiving laboratory and the receiving individual are qualified to accept HRPT materials.

If temporary storage needs to be provided while packages are being held in shipping and receiving areas or during transit, the security should be equivalent to that for an Exclusion Area used for handling HRPT. The responsible official at the sending laboratory should verify that the intended carrier is able to provide this level of security.

The sending laboratory should initiate a chain-of-custody procedure that documents the control of the package containing HRPT materials during its transit and ensures the secure receipt of the material at the receiving facility. The receiving laboratory should provide notification of successful receipt to the sending facility. The sending laboratory should notify the receiving laboratory promptly of the time that the shipment left the sending laboratory. Both laboratories should be prepared to independently follow up immediately if any shipment does not arrive as expected. At the same time, the incident should be reported to a higher authority.

C.5 ERPT

C.5.1 Physical Security

C.5.1.1 Special Exclusion Areas

A Special Exclusion Area resides within a Limited Area and is intended for the storage and use of ERPT and for the management of laboratory animals infected with an ERPT. A Special Exclusion Area, like an Exclusion Area, has barriers that identify the boundaries and encompass the designated space as well as access controls and intrusion detection to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area without escort.

Access to a Special Exclusion Area requires a unique item and unique knowledge, such as a physical key and positive identification provided by a guard or an electronic key and a PIN. It is highly recommended that the Special Exclusion Area and the surrounding Limited Area have access controls and intrusion detection systems that are electronic and monitored by an on-site guard force that is equipped to respond to any alarms in these areas.

C.5.2 Personnel Management

C.5.2.1 Screening

Personnel with direct access to ERPT are in the High Risk position category. Employees with access to ERPT should receive a more comprehensive background investigation than those with access to HRPT, and the background investigation should be updated on a periodic basis, typically every 5 or 10 years.

Institutions that hold ERPT may consider incrementally increasing the background checks for all personnel at the facility, including those in Low Risk positions. The risk associated with these pathogens and toxins is such that extra precautions are generally warranted for all personnel who have authorized, unescorted access to the facility.

C.5.2.2 Visitors

Escorting unauthorized personnel, such as visitors, into a Special Exclusion Area should not be permitted: only persons who are fully authorized should be permitted to enter. Full authorization may only occur after all personnel management procedures are complete, including background investigation and evaluation. In other words, no visitors or regular employees who would qualify for an interim authorization for a restricted area should be allowed into a Special Exclusion Area. If maintenance of the Special Exclusion Area is required, all ERPT should be removed in advance. Entry of delivery and custodial personnel should be prohibited.

C.5.3 Material Control and Accountability

Laboratory management should keep a record of where ERPT materials are stored and used and a record of the corresponding accountable scientists. Laboratory notebooks maintained by accountable scientists should document the stocks and use of ERPT materials. Notebooks should not leave the Special Exclusion Areas without special measures to ensure information security. Such measures should be approved in advance by the responsible facility official.

Inventories should be maintained in secure, limited-access databases that are consistent throughout the facility. Databases must be secure from unauthorized disclosure, and information should be carefully protected against loss or alteration, whether by accidental or malicious means. Limited access to the databases would be controlled separately for read, write, or change permissions, and these access permissions would be part of the MCA information log.

The transfer of ERPT should be documented both in notebooks and in the laboratory inventory database. Paper documentation of such a transfer, such as carrier receipts, should be kept for historical documentation of the transfer.

Transfer should be authorized and approved by the facility's biosafety officer or by another designated responsible official before the material ships. It is the responsibility of this designated responsible official of the sending laboratory to confirm that both the receiving laboratory and the receiving individual are qualified to accept the ERPT materials.

ERPT should be shipped only via a carrier who understands the risk to the asset and has a transportation security plan. If temporary storage needs to be provided for packages awaiting transit or during transit, the security should be equivalent to that for the restricted area designated for handling ERPT. The responsible official at the sending laboratory must verify that the intended carrier is qualified to provide this level of security.

Both the sender and the recipient involved in the transfer should be authorized to handle the particular ERPT. The originating laboratory should initiate a chain-of-custody procedure that documents the control of the package containing ERPT materials during its transit and ensures the secure receipt of the material at the receiving facility. The receiving laboratory should provide notification of successful receipt to the sending facility. The originating laboratory should notify the receiving laboratory promptly when the material ships. Both laboratories should be prepared to independently follow up immediately if any shipment does not arrive as expected. At the same time, the incident should be reported to a higher authority.

Packaging of ERPT materials for transfer that involves custody by commercial carrier should include tamper indication that would reveal breach of containment integrity during shipment. The sending laboratory should be qualified to apply such tamper indication, and the receiving laboratory should be qualified and prepared to inspect and assess the tamper indication. Any indication of actual or possible breach of containment is an anomaly that should be reported and is subject to follow-up investigation.

This page intentionally left blank.

Appendix D. Adversary Descriptions

D.1 Adversaries

Potential adversaries can be organized based on their level of access to the asset that might be stolen. *Insiders* have authorized access to the site and/or facility and may or may not have direct, authorized access to the asset. *Outsiders* are individuals without authorized access to the site or facility.

In general, the most significant threat to a facility's biological assets is the insider who has authorized access to the asset. This form of adversary has a significant level of technical expertise, knowledge of operations, access to the materials, and the ability to act covertly, all of which reduces the risk to the individual and increases the likelihood of success. The outsider, who is without many if not all of these advantages, could isolate pathogenic material from nature or acquire it from a variety of unprotected biomedical research institutes, clinical facilities, biotechnology industries, or culture collections around the world¹⁹ rather than incur the risk of detection and diminished likelihood of success that would result from attacking a laboratory that has implemented a biosecurity system.

D.1.1 Adversary Spectrum

The types of individuals or groups included in the adversary spectrum represent a set of *possible* adversaries. These adversary descriptions are not intended to imply that all members of a group of individuals who have legitimate business at a facility will attempt to steal biological agents or other assets but are included to simply describe a specific range of possibilities. In order to analyse an adversary's contribution to the risks a facility faces, it is necessary to specifically define each adversary. Should a facility reside in a region that has a particular type of adversary with a mixture of attributes not specifically listed below, a new adversary description should be created and the risk that adversary poses to the facility evaluated.

Not all of these adversary descriptions will apply to all facilities. The insider category, for instance, may be subdivided in order to address the possibility that a facility has access restrictions that separate its population. It is common to have only two insider categories: an *Insider with Full Access* and an *Insider without Full Access*, indicating that a laboratory area may have restrictions on who is permitted inside the laboratory itself but that the remainder of the facility is open to those who work or who conduct business there. It is also possible that there is only one insider category, the *Insider*, for facilities that do not restrict access to any portion of the facility. The types of outside adversaries should also be reviewed, and attention should be given to each attribute, especially to the adversary's motivation and tools. Each facility should tailor these categories appropriately.

¹⁹ The one exception is the Variola major virus, the causative agent of smallpox, which has been globally eradicated. The two official repositories are the Centers for Disease Control and Prevention, Atlanta, Georgia (U.S.) and the State Research Institute for Virology and Biotechnology, Koltsovo (Russia).

D.1.1.1 Insiders

Insiders may be broken down into different adversary descriptions based on their level of access, but they will have some characteristics in common. The insider as an adversary may be motivated by disgruntlement, psychological imbalance, or the desire to commit a terrorist act. The intent of the malevolent insider is to steal or destroy an asset without detection. The insider would be expected to abort any theft attempt to avoid identification and is nonviolent. An insider has the opportunity to choose the best time to commit a malevolent act.

D.1.1.1.1 Insider with Full Access

The *Insider with Full Access* may be a laboratory worker or other individual who has unescorted access to the asset being evaluated. He or she has scientific and operational knowledge and authorized access. Authorized access affords this person extensive knowledge of the facility and operating systems.

D.1.1.1.2 Escorted Insider with Full Access

The *Escorted Insider with Full Access* includes, for instance, an invited colleague or a working visitor who has the intent to steal intellectual property and/or acquire an asset. This insider has direct but supervised access to the asset; may have system knowledge that can be used to his or her advantage; and may have limited, authorized access to the facility.

D.1.1.1.3 Insider with Building Access

The *Insider with Building Access* is an insider who could hold any one of many insider positions not directly associated with the asset. He or she has operational knowledge and authorized access to the site and to some buildings.

D.1.1.1.4 Insider with Site Access

The *Insider with Site Access* may be an invited trades professional, including a specialized technician such as an electrician or a plumber, as well as a delivery person or any other service person authorized to be on-site on an irregular basis. As an adversary, this individual has the intent to steal or destroy an asset, to sabotage operations, or to disrupt scientific achievements. This individual may have system knowledge that can be used to his or her advantage and may have authorized access to the facility and its assets.

D.1.1.2 Terrorist Group

Terrorist groups are usually well funded and may be supported by states, religious groups, individuals, or even organized crime. Because such groups are well funded, they are generally well equipped, trained, and able to rehearse an attack. Terrorists may be highly organized. Their motivation may be to cause mass casualties, an economic crisis, or widespread fear or it may be

to make a political statement or effect change within a corporation or an entity such as a government. Terrorists have been shown to be violent and willing to die.

D.1.1.3 Single Terrorist

A *Single Terrorist* may be well equipped, trained, and able to rehearse. The Single Terrorist's motivation may be to make a political statement, to express anger, or to steal a high-consequence asset in order to ultimately achieve his or her goals. The Single Terrorist is willing to use violence and force.

D.1.1.4 Psychotic Outsider

The *Psychotic Outsider* may have motivations that seem convoluted and perhaps pathological because of a mental or behavioural disorder. This disorder may cause gross distortion of a person's perception of reality and ability to communicate. This person does not have authorized access to the facility. This person has no specific familiarity with the facility, its assets, or its protection systems. The Psychotic Outsider is possibly armed with a handgun but is not homicidal (intends only to threaten use of the weapon) and is not willing to risk death.

D.1.1.5 Extremists

Extremists may operate individually or in groups. The intent of Extremists is to make a political statement or to express protest. Their usual tactics are to march, picket, occupy property, or commit violence against an institution. Motivation is based on opposition to programmes for ecological, political, economic, or other reasons. Extremists have general information about the facility but not specific information about the location of the assets or the facility's protection systems.

Extremists are possibly armed with handguns but are not homicidal (they intend only to threaten use of a weapon; however, collateral loss of human life is possible in the event arson is employed) and are not willing to risk death. No member of the group has authorized access to the facility. Their intent is to protest the institution's activities, and they may destroy property or release animals. They do not intend to steal an asset or to release pathogens into the environment; however, their acts may inadvertently cause a release of pathogens into the environment.

D.1.1.6 Criminals

The motivation of the *Criminal* is financial gain. The Criminal acts alone and may use weapons and hand tools to achieve his or her objective. In extreme cases this adversary is affiliated with organized crime.

D.1.1.7 Vandalism

Vandals may operate individually or in groups. Their motivation is to cause a nuisance by damage or destruction. Tools range from spray paint to knives and hand tools and may include guns if the vandals are also target shooters or hunters. Vandals tend to attack facilities in the vicinity of their homes and are not homicidal.

DISTRIBUTION:

1 Deborah Ozga
International Policy and Analysis Division
Forrestal Building, GA-007
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585-0440

1 Scott Davis
(NA-241)
International Policy and Analysis Division
Forrestal Building, GA-007
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585-0440

1	MS 1361	Kimberly Silver	6923
1	MS 1363	Terri Olascoaga	6920
1	MS 1371	Natalie Barnett	6928
1	MS 1371	Susan Caskey	6928
1	MS 1371	Jennifer Gaudio	6928
1	MS 1371	Lauren Hickok	6928
1	MS 1371	Robert Huelskamp	6926
1	MS 1371	John Milloy	6928
1	MS 1371	Susan Rivera	6928
1	MS 1371	Reynolds Salerno	6928
1	MS 1371	Michelle Zamora	6928
1	MS 1373	George Baldwin	6924
1	MS 1375	Dori Ellis	6900
1	MS 1378	Kathleen Lowe	6929

1 MS 9018 Central Technical Files, 8523-1
5 0899 Technical Library, 4414

This page intentionally left blank.